DIGITALICA

Ugo Pagallo

# Il diritto nell'età dell'informazione

## Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti


G. Giappichelli Editore – Torino

DIGITALICA

*Collana diretta da* UGO PAGALLO

12

*La collana presenta al lettore italiano una serie di studi interdisciplinari in informatica, diritto e nuove tecnologie, con la traduzione di importanti contributi di matematica, computer science, teoria generale del diritto, filosofia cognitiva, etc., oltre a opere nazionali particolarmente attente alle nuove frontiere tenologiche degli ordinamenti giuridici, politici ed economici contemporanei. La cifra teoretica è data dagli assunti della cosiddetta digital philosophy che, a partire dalle opere di Kurt Gödel e Alan Turing fino agli odierni dibattiti sull'intelligenza artificiale, i computer quantistici, la realtà "aumentata" e "virtuale", i sistemi esperti, trova nella tradizione pitagorico-platonica e, soprattutto, nel pensiero di Leibniz, le proprie origini storiche.*

Ugo Pagallo

# Il diritto nell'età dell'informazione

## Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti


G. Giappichelli Editore – Torino

G. GIAPPICHELLI EDITORE - TORINO – 2014
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-348-5835-6

*The research leading to these results was funded by the University of Torino under the agreement with the Compagnia di San Paolo "Progetti di Ateneo 2011" and the title of the Project is "The Making of a New European Legal Culture. Prevalence of a single model, or cross-fertilisation of national legal traditions?" Academic coordinator Prof. Michele Graziadei*

*La presente pubblicazione è frutto della ricerca svolta nell'ambito del Progetto di Ateneo 2011 dal titolo: "The Making of a New European Legal Culture. Prevalence of a single model, or cross-fertilisation of national legal traditions?". Coordinatore scientifico Prof. Michele Graziadei. Il progetto è finanziato dalla Compagnia di San Paolo.*

# *Indice*

*pag.*

*pag.*

# *Indice delle figure*

# *Indice delle tavole*

# *Indice degli acronimi*

**ACLU** = Associazione statunitense per la tutela delle libertà civili (da *American Civil Liberties Union*)

**ACTA** = Accordo (mancato) sulla contraffazione nel commercio (da *Anti-Counterfeiting Trade Agreement*)

**AGCOM** = Autorità italiana per le garanzie nelle comunicazioni

**BBC** = La RAI britannica, ma molto più autorevole (da *British Broadcasting Company*)

**BCR** = Schema di regole vincolanti per le imprese (da *Binding Corporate Rules*)

**CBS** = Canale televisivo statunitense (da *Columbia Broadcasting System*)

**CCTV** = Telecamere a circuito chiuso (da *Closed Circuit Television*)

**CDA** = Legge statunitense sul decoro nelle comunicazioni (da *Communications Decency Act*)

**CE** = Comunità europea

**CECA** = Comunità europea del carbone e dell'acciaio

**CEDU** = Convenzione (e/o corte) europea dei diritti dell'uomo

**CEE** = Comunità economica europea

**CEO** = Amministratore delegato (da *Chief Executive Officer*)

**CERN** = Organizzazione europea per la ricerca nucleare (dal francese *Conseil Européen pour la Recherche Nucléaire*)

**CFC** = Clorofluorocarburi

**CSS** = Fogli di stile informatici (da *Cascading Style Sheets*)

**DDR** = L'ex Germania dell'est o Repubblica Democratica Tedesca (da *Deutsche Demokratische Republik*)

**DEA** = Legge britannica sull'economia digitale (da *Digital Economy Act*)

**DHS** = Ministero statunitense per la sicurezza nazionale (da *Department of Homeland Security*)

**DMCA** = Legislazione statunitense sul copyright (da *Digital Millennium Copyright Act*)

**DNA** = Acido desossiribonucleico o deossiribonucleico (da *Deoxyribonucleic Acid*)

**DNS** = Sistema dei nomi a dominio in rete (da *Domain Name System*)

**DoS** = Attacco informatico volto a impedire i servizi in rete (da *Denial of Service*)

**DRM** = Gestione dei diritti digitali (da *Digital Rights Management*)

**DVD** = Dischi versatili digitali

**ECPA** = Legge statunitense sulla privacy per le comunicazioni elettroniche (da *Electronic Communications Privacy Act*)

**EDPS** = Supervisore europeo della protezione dati (da *European Data Protection Supervisor*)

**EFF** = Associazione statunitense per i diritti digitali e la libertà di parola (da *Electronic Frontier Foundation*)

**ENEL** = Ente nazionale per l'energia elettrica

**ETNO** = Associazione degli operatori europei per la rete di telecomunicazioni (da *European Telecommunications Network Operators*)

**EURATOM** = Comunità europea dell'energia atomica

**FAQ** = Domande fatte di frequente (da *Frequently Asked Questions*)

**FBI** = Agenzia federale statunitense (da *Federal Bureau of Investigation*)

**FIP** = Pratiche commerciali d'informazione leale (da *Fair Information Practices*)

**FISA** = Legge statunitense sulla sorveglianza e l'intelligenza all'estero (da *Foreign Intelligence Surveillance Act*)

**FISC** = Tribunale statunitense per la sorveglianza e l'intelligenza all'estero (da *Foreign Intelligence Surveillance Court*)

**FMI** = Fondo monetario internazionale

**FTC** = Agenzia statunitense per il commercio (da *Federal Trade Commission*)

**GATT** = Accordo generale sulle tariffe e il commercio (da *General Agreement on Tariffs and Trade*)

**GCHQ** = Agenzia britannica d'intelligenza (da *Government Communications Headquarters*)

**GNI** = Iniziativa per la rete globale (da *Global Network Initiative*)

**GPS** = Sistema di posizionamento satellitare globale (da *Global Positioning System*)

**HIPPA** = Legislazione statunitense sull'assicurazione sanitaria e protezione dei dati (da *Health Insurance Portability and Accountability Act*)

**HRI** = Interazione tra uomini e robot (da *Human-Robot Interaction*)

**HTTPS** = Applicazione crittografica asimmetrica (da *HyperText Transfer Protocol over Secure Socket Layer*)

**IAB** = Consiglio per l'architettura d'internet (da *Internet Architecture Board*)

**IANA** = Autorità per l'assegnazione dei numeri su internet (da *Internet Assigned Numbers Authority*)

**ICANN** = Ente per l'assegnazione dei nomi e numeri su internet (da *Internet Corporation for Assigned Names and Numbers*)

**ICC** = Corte penale internazionale (da *International Criminal Court*)

**ICT** = Tecnologia dell'informazione e comunicazione (da *Information and Communication Technology)*

**IEEE** = Istituto degli ingegneri elettrici ed elettronici (da *Institute of Electrical and Electronics Engineers*)

**IETF** = Unità di lavoro degli ingegneri per internet (da *Internet Engineering Task Force*)

**IGF** = Assemblea per la governance d'internet (da *Internet Governance Forum*)

**IP** = Indirizzo su internet (da *Internet Protocol access*)

**IPsec** = Standard a pacchetto in rete per la sicurezza (da *IP security*)

**ISOC** = Società internet (da *Internet Society*)

**ISP** = Fornitori di servizi su internet (da *Internet Service Providers*)

**ITS** = Sistemi di trasporto intelligente (da *Intelligent Transport System*)

**ITU** = Unione internazionale delle telecomunicazioni (da *International Telecommunication Union*)

**NAACP** = Associazione statunitense per la difesa della gente di colore (da *National Association for the Advancement of Colored People*)

**NATO** = Organizzazione militare fondata sul trattato dell'Atlantico nord (da *North Atlantic Treaty Organization*)

**NBC** = Canale televisivo statunitense (da *National Broadcasting Company*)

**NGO** = Organizzazioni e associazioni non governative (da *Non-Governmental Organization*)

**NPR** = Radio pubblica statunitense (da *National Public Radio*)

**NSA** = Agenzia statunitense di sicurezza (da *National Security Agency*)

**OCSE** = Organizzazione per la cooperazione e sviluppo economico

**OGM** = Organismo geneticamente modificato

**ONU** = Organizzazione delle nazioni unite

**P2P** = Pari a pari (da *Peer to Peer*, o sistemi informatici di condivisione in rete)

**PIL** = Prodotto interno lordo

**PNR** = Registri del nome dei passeggeri (da *Passenger Name Records*)

**PPP** = Partenariato pubblico privato

**PSI** = Informazione del settore pubblico (da *Public Sector Information*)

**RFID** = Congegni per l'identificazione a radio-frequenze (da *Radio Frequency Identification*)

**RPA** = Velivoli pilotati in remoto (da *Remotely Piloted Aircrafts*)

**SABAM** = Omologa belga della società italiana degli autori ed editori, o SIAE

**SNS** = Servizi per piattaforme sociali (da *Social Network Services*)

**SSL** = Protocollo crittografico (da *Secure Sockets Layer*) poi sostituito dai TLS

**SSH** = Protocollo per sessioni remote cifrate in rete (da *Secure SHell*)

**TBT** = Barriere tecniche al commercio (da *Technical Barriers to Trade*)

**TCP** = Protocollo per il controllo della trasmissione delle informazioni in rete (da *Transmission Control Protocol*)

**TFUE** = Trattato sul funzionamento dell'Unione europea

**TKG** = Leggi federale tedesca sulle telecomunicazioni (da *Telekommunikationsgesetz*)

**TLS** = Protocollo crittografico (da *Transport Layer Security*) seguìti agli SSL

**UAV** = Sistemi di volo senza pilota (da *Unmanned Aircraft Systems*)

**UDRP** = Politica per la risoluzione uniforme delle controversie (da *Uniform Dispute Resolution Policy*)

**UE** = Unione europea

**UNCITRAL** = Commissione delle Nazioni Unite sul diritto internazionale commerciale (da *United Nations Commission on International Trade Law*)

**USA** = Stati Uniti d'America (da *United States of America*)

**USC** = Il codice statunitense federale (da *United States Code*)

**VHS** = Sistemi video domestici (da *Video Home System*)

**W3C** = Consorzio per il world wide web (da *World Wide Web Consortium*)

**WCIT** = Conferenza mondiale sulle telecomunicazioni internazionali (da *World Conference on International Telecommunications*)

**WIPO** = Organizzazione mondiale a tutela della proprietà intellettuale (da *World Intellectual Property Organization*)

**WPFC** = Comitato mondiale per la stampa libera (da *World Press Freedom Committee*)

**WP 29** = Autorità garanti europee della protezione dati (da *Article 29 Working Party*)

**WTO** = Organizzazione mondiale del commercio (da *World Trade Organization*)

# *Prefazione*
## *(sul lupo, l'agnello e il pinguino)*

"Il lupo incolpa sempre l'agnello per intorbidirgli il fiume" (Elihu Root)

"Le cose cambiano" (Il Pinguino di Batman – Il Ritorno)

Il primo consiglio che mi sento di dare allo studente, o ricercatore, che si prepara a svolgere la propria tesi di laurea o di dottorato, è di chiarire (a se stessi e agli altri) quale sia il problema. La tesi non è infatti che la risposta – o, appunto, la tesi – che l'autore intende dare al problema, o all'insieme di problemi, oggetto della ricerca. La risposta andrà poi articolata in un insieme di argomentazioni che, a loro volta, presentate in capitoli e paragrafi, presuppongono la definizione preliminare dei concetti in gioco.

La raccomandazione ha ovviamente natura riflessiva, nel senso che si applica anche, se non soprattutto, a chi quel consiglio lo da; per cui, a ben vedere, qual è mai il problema che anima questo libro?

La tesi è che siamo soltanto all'inizio di una rivoluzione epocale, la quale trova nel concetto d'informazione l'elemento cruciale che propone, solleva o crea una serie di sfide e questioni inedite al mondo del diritto.

Come punto di partenza, qualche cifra non guasta. Secondo alcuni autorevoli studi di statistica[1], già nel 2010 le spese d'intrattenimento, giochi e media hanno superato quelle militari: 2 mila miliardi di dollari contro 1.74 mila miliardi. Sebbene la parte del leone spetti alle spese per il servizio sanitario latamente inteso (6.5 mila miliardi), quelle per l'intrattenimento e i media vanno crescendo sistematicamente, passando dal 26% della spesa totale nel 2011 al 33.9% previsto per il 2015. Questi flussi monetari vanno strettamente ricondotti e si sovrappongono agli investimenti nel settore delle tecnologie dell'informazione e comunicazione (ICT): nell'anno in cui le spese per l'intrattenimento, i giochi e i media hanno superato quelle militari, lo stanziamento per le ICT è stato di ben 3 mila miliardi di dollari. Rinviando il lettore a ulteriori indicazioni quantitative nel corso del libro, ben può dirsi sin d'ora che non possiamo staccare il mondo dall'uso delle ICT, se non per paralizzarlo del tutto. Per la prima volta nella storia dell'umanità, siamo di fronte a società che non

[1] Il richiamo va all'Istituto internazionale di Stoccolma per la ricerca sulla pace (*Stockholm International Peace Research Institute*), al *PricewaterhouseCoopers* e all'*International Data Corportation* (IDC): i dati sono disponibili in rete. Ulteriori dettagli in Floridi (2014: 97).

solo impiegano le ICT, come la scrittura o la stampa, a proprio uso e consumo; ma dipendono da queste tecnologie e, in genere, dal trattamento e flusso dell'informazione come propria risorsa vitale. In che modo questo nuovo scenario incide, dunque, sul mondo del diritto?

A questo fine, torna utile una favola del grande scrittore greco Esopo (620-564 a.C.), vale a dire la storia del lupo che, avendo visto un agnello abbeverarsi nei pressi di un torrente, decise di divorarselo con una qualche scusa. Appostatosi a monte di dove si trovava l'agnello, il lupo contestò al mansueto animale il fatto che gli stesse intorbidendo l'acqua. L'agnello però rispose che, stando a valle, gli era impossibile sporcare l'acqua al lupo. Al che, venuto meno quel pretesto, il lupo pensò bene di accusare l'agnello di avergli insultato il padre l'anno prima; ma, questa volta, l'agnello fece presente che, in realtà, l'anno prima egli non era ancora nato. "Bene", concluse il lupo, "se tu sei così bravo a trovare delle scuse, io non posso mica rinunciare a mangiarti".

Una volta che sostituiamo l'acqua del racconto con il concetto d'informazione, la favola risulta altamente istruttiva per iniziare a cogliere la serie di sfide con cui è chiamato a misurarsi oggi il diritto. Tanto nel caso del torrente di Esopo quanto con il concetto d'informazione, abbiamo infatti a che fare con una risorsa abbondante, e non scarsa; la quale si presta a giochi vantaggiosi per tutti, e non a somma zero. Basti pensare a come, nell'era predigitale, quando si prestavano libri e dischi agli amici, l'atto stesso del prestare comportava che ci si privasse della propria copia del libro o del disco. Non a caso, all'atto della consegna si accompagnava spesso, scherzosamente, il detto "san Pietro torna indietro". Invece, l'idea stessa del prestare è venuta meno con il formato elettronico di un bene informazionale come un libro o un disco, trasformandosi piuttosto in una nuova forma di condivisione o dono digitale: il fatto che io ceda le informazioni contenute in un libro elettronico, o in un brano musicale in mp3, non mi priva certo di quelle stesse risorse informazionali. Mentre la tradizionale versione cartacea di questo libro implica l'alternativa posta dal lupo nel racconto di Esopo, per cui o il libro ce l'ho io, oppure tu, la versione elettronica di questo stesso volume si addice all'argomento dell'agnello, per cui il fatto che si disponga di quelle informazioni o ci si abbeveri alla fonte della cultura in questo caso, non sottrae alla disponibilità del lupo né un bit di informazione, né una goccia d'acqua. Si ha in sostanza a che fare con le leggi di un nuovo mondo – imperniato sulle tecnologie dell'informazione e della comunicazione – rese popolari nel 1996 con la "Dichiarazione d'indipendenza del Cyberspazio" di John Perry Barlow (n. 1947). La tesi di Barlow, a cui, peraltro, dobbiamo alcune delle più acide canzoni nella storia del rock psichedelico degli anni sessanta e settanta con il gruppo "Grateful Dead", è che l'insieme delle regole e dei principi invalsi nell'epoca predigitale e imperniati sulla logica a somma zero del lupo nella favola di Esopo, dovrebbero stare alla larga del nuovo mondo di valori comunitari propri del cyberspazio.

Nel corso degli ultimi vent'anni, bisogna del resto ammettere che si sia assistito all'emersione di una pletora d'ordini spontanei e a inedite forme di cooperazione sociale nei più svariati campi dell'industria e del commercio, della ricerca tecnologica e della cultura. Uno dei massimi esperti del settore, Yochai Benkler (n. 1964), professore di diritto all'università di Harvard, ha riassunto le tendenze in atto con il

titolo di un volume pubblicato nel 2011, *Il pinguino e il leviatano: il trionfo della cooperazione sull'egoismo*. Dopo il lupo e l'agnello della favola di Esopo, l'emblema della trasformazione sarebbe infatti il pinguino di Linux, vale a dire la famiglia di sistemi operativi "open source" nel campo dell'informatica, sviluppati fin dai primi anni novanta del secolo scorso secondo un'ottica collaborativa, e non proprietaria; ossia, libera e aperta, e non vincolata alla logica del profitto. Tra gli esempi ulteriori proposti da Benkler, vanno aggiunti Wikipedia, la nota enciclopedia online; le forme d'organizzazione aziendale e i rapporti di lavoro, fondati sulla fiducia e ampi margini d'autonomia, della Southwest Airlines; la rete intessuta dalla Toyota con la propria catena di fornitori; il modello di prevenzione del crimine adottato dalla città di Chicago; e altro ancora. Ciò che questi esempi illustrano, a giudizio del giurista americano, è come nell'età dell'informazione, in ciò che Benkler ha altrimenti definito come la "ricchezza delle reti", la cooperazione vada trasformando gli affari e il commercio, gli stati e la società, "perché oggi, quando i costi della collaborazione sono diventati più bassi di quanto mai lo siano stati precedentemente, non esistono limiti a ciò che si può ottenere lavorando assieme".

Eppure, anche ad ammettere la bontà dell'analisi di Benkler e nonostante le proprietà ontologiche dei beni informazionali, bisogna sottolineare come le cose siano andate spesso nel senso del lupo, più che dell'agnello o del pinguino; e cioè, fuor di metafora, come anche nell'età dell'informazione sia spesso invalsa una logica rivale a somma zero, piuttosto che la mistica della comunione digitale preconizzata da Barlow nel suo manifesto. Perché?

Una prima risposta è suggerita proprio dai processi di trasformazione in corso e dall'ovvia resistenza di chi rischia di essere messo fuori gioco dal passaggio dalla società industriale all'età dell'informazione, e difende a spada tratta i vecchi modelli organizzativi. L'esempio dei libri e dei dischi, fatto in precedenza, ne è un'ottima dimostrazione: ciò che prima ho presentato come una nuova forma di condivisione o dono digitale, è invece interpretato dai detentori dei diritti di proprietà intellettuale come una forma di pirateria digitale o furto. Secondo quest'ultima prospettiva, la logica a somma zero proposta dal lupo nella favola di Esopo deve (essere fatta) valere a prescindere dal formato, elettronico o meno, di un oggetto informazionale come questo libro o un brano musicale, su cui l'editore, più che l'autore, vanta diritti d'esclusiva nel mondo reale, su internet, o nel cyberspazio. A dar manforte al lupo ci ha poi pensato il Leviatano di Benkler nel corso degli ultimi vent'anni, con una fitta serie di accordi internazionali e di normative nazionali con cui i legislatori degli stati sovrani hanno pensato di fronteggiare la rivoluzione in corso e puntellare il passato. Sebbene non siano mancati nuovi modelli di distribuzione e condivisione dei beni informazionali anche nel campo dell'editoria e dello spettacolo, siamo ben lungi dall'aver trovato un soddisfacente equilibrio tra il buon senso dell'agnello, le istanze del pinguino e le esigenze del lupo.

Inoltre, occorre distinguere due tipi d'informazione. Alla logica della condivisione proposta dall'agnello nella favola di Esopo, per cui l'accento cade sui fattori dai quali tale apertura dipende – come nel caso della disponibilità delle informazioni, con le condizioni della sua accessibilità, e via dicendo – vanno affiancate le norme e i principi che non solo legittimano le restrizioni nel flusso delle informazioni; ma che a loro volta ripropongono, con buona pace dell'agnello, una logica rivale, anta-

gonista o proprietaria. Anche nell'età dell'informazione, in fin dei conti, esistono dati dotati di significato, e cioè, appunto, informazioni che richiedono di rimanere riservate o segrete, tanto sul piano pubblico (es. segreti di stato), quanto nel settore privato (es. privacy personale). A ciò si aggiunga che molte informazioni che una volta erano disponibili al pubblico e, come tali, destinate a essere aperte, possono diventare problematiche nel nuovo ambiente elettronico. È il caso delle copie dei giornali conservati nelle biblioteche comunali che, riversate nelle banche dati dei quotidiani su internet, hanno fatto tornare alla ribalta, sotto nuove vesti, il cosiddetto diritto all'oblio. La logica a somma zero del lupo nella favola di Esopo viene di qui fatta valere da ogni individuo che si avvalga del diritto riconosciutogli dalla Corte di giustizia europea il 13 maggio 2014, per sottrarre agli altri la disponibilità delle notizie che lo riguardano, indipendentemente dal danno che tali notizie possano arrecare. Al pari dei modelli per la distribuzione e condivisione dei beni informazionali cui si è fatto cenno in precedenza, anche in questo caso siamo ben lungi dall'aver trovato un equilibrio tra le norme e principi chiamati a restringere o agevolare i flussi dell'informazione. Si presti attenzione all'odierno dibattito sui dati aperti e la tutela dei dati personali; oppure, tra il diritto a "prendere parte liberamente alla vita culturale della comunità, di godere delle arti e di partecipare al progresso scientifico e ai suoi benefici" – come solennemente dichiarato dal primo comma dell'articolo 27 della Dichiarazione universale dei diritti dell'uomo – e il "diritto alla protezione degli interessi morali e materiali derivanti da ogni produzione scientifica, letteraria e artistica", garantiti dal secondo comma dello stesso articolo.

Questa tensione tra la logica proprietaria o a somma zero del lupo nella favola di Esopo, e la logica della condivisione dell'agnello o del pinguino, può essere finalmente ricondotta al pessimismo antropologico di fondo suggerito a conclusione del racconto, per cui, con le parole di Esopo, "la favola dimostra che contro chi ha deciso di fare un torto non c'è giusta difesa che tenga". L'idea sarebbe stata in séguito riassunta dal commediografo romano Plauto (255-250/184 a.C.), con la nota formula dell'*homo homini lupus*, ripresa e ulteriormente perfezionata dai più illustri esponenti del pensiero giuridico e politico moderno, a partire da chi oggi ne è ritenuto il padre, ossia Thomas Hobbes (1588-1679). Avendo a mente i nuovi scenari dell'età dell'informazione, ben può darsi che Benkler abbia visto giusto ne *Il Pinguino e il Leviatano*, quando insiste su come sia i presupposti sia le conclusioni del discorso di Hobbes sarebbero stati messi in mora nell'odierno quadro di società che dipendono dall'uso delle tecnologie dell'informazione e della comunicazione come propria risorsa vitale. Revocata in dubbio la logica a somma zero dello stato ferino degli uomini allo stato di natura con le nuove esperienze delle risorse aperte (*open source*) e del software libero, con forme di collaborazione scientifica e commerciale fondate sull'autonomia degli individui e la fiducia, con l'emersione a getto continuo di forme spontanee d'ordine nel cyberspazio, verrebbero anche meno le tesi di Hobbes sul principio di sovranità e il monopolio dello stato sulle fonti del diritto, sul principio di coattività delle leggi e l'ordine internazionale come un mero aggiornamento della favola di Esopo su scala planetaria.

I problemi tuttora aperti tra le norme e i principi chiamati ora a restringere ora ad agevolare i flussi dell'informazione nelle odierne società complesse, stanno a suggerire come non sia tuttavia il caso di sostituire semplicemente il Leviatano di

Hobbes con il Pinguino di Benkler e, se per questo, il lupo di Esopo con l'agnello. Piuttosto, occorre comprendere come le dinamiche del potere siano destinate a ripresentarsi nonostante l'uso di risorse all'apparenza abbondanti e non rivali, come nel caso dei beni informazionali, per cui il problema è, se mai, di appurare come il potere sia oggi redistribuito tra nuovi e vecchi attori sociali, rimanendo del pari aperta l'ulteriore questione di stabilire il ruolo che il diritto svolge in questi casi. Anche a restringere il fuoco dell'analisi alla secca alternativa tra la logica del lupo e dell'agnello sul piano delle scelte legislative, scopriremmo infatti non due, ma quattro distinti scenari:

i) l'intervento normativo funzionale alla logica dei lupi e del potere, come suggeriscono certe varianti del realismo giuridico;
ii) l'azione del diritto a tutela dei più deboli, come proposto invece da certa tradizione giusnaturalista e costituzionalista;
iii) la tutela dei più deboli volta a renderli a loro volta lupi, secondo la logica dei giochi a somma zero vista già in azione con il cosiddetto diritto all'oblio;
iv) l'opera del legislatore teso a bilanciare i diversi interessi in gioco sulla base di criteri di proporzionalità e ragionevolezza.

A complicare le cose, bisognerebbe poi aggiungere sia i diversi piani d'intervento nazionale e internazionale, sia i distinti settori dell'ordinamento, tra diritto costituzionale, penale, civile, amministrativo, ecc., sia, soprattutto, il fatto che l'intervento del legislatore non opera in una sorta di vuoto normativo, ma concorre con altre e ulteriori forme di regolazione sociale come le norme e pratiche di una comunità, le consuetudini, le forze del mercato o la tecnologia. Soltanto avendo a mente tutti questi parametri, saremo in grado di dar conto del riposizionamento in atto nel mondo del diritto, nella nuova età dell'informazione. Prima d'iniziare a introdurre il lettore al modo in cui l'indagine del presente volume è stata strutturata, come in ogni prefazione, è giunto il momento dei ringraziamenti.

*****

L'intento del libro non è certo quello di esaurire nel dettaglio tutti gli aspetti del diritto nell'età dell'informazione ma, piuttosto, di spiegare come il diritto stia mutando nella nuova era. Per cogliere la profondità del cambiamento, bisognerà naturalmente soffermarsi su ciò che, ereditato dalla tradizione, va trasformandosi. Questa prospettiva consentirà di selezionare della sterminata mole d'istituti, tecniche e forme organizzative del diritto, quegli aspetti dell'ordinamento che mettono in risalto e chiariscono l'entità della variazione. Anche a restringere in questo modo il proprio punto di vista, tuttavia, l'oggetto di studio appare complesso e intricato, attraversando i settori della filosofia e la teoria generale del diritto, il diritto civile e il penale, il costituzionale e l'internazionale, la storia del diritto, la sociologia giuridica e il diritto comparato. Questo spiega perché, senza i consigli, commenti e critiche degli amici, colleghi ed esperti dei diversi settori qui indagati, queste pagine non sarebbero state possibili. Un sentito ringraziamento va in particolare a Carlo Blengino, Raffaele Caterina, Massimo Durante, Luciano Floridi, Michele Graziadei, Valeria Marcenò e Monica Senor, nonché a mio padre per le puntuali osservazioni pro-

poste nel corso della stesura finale del libro. Sono conscio che, nonostante questi apporti, possano essere rimaste ambiguità o imprecisioni. Ciò semplicemente vuol dire che non ho tratto sufficiente profitto dalle ore passate con loro a discutere questo o quell'aspetto della ricerca. Infine, sono grato a Giuliano Giappichelli per aver creduto nella versione "open access" del presente volume, e a Paola Alessio e Francesca Leva per la produzione editoriale.

Torino, settembre 2014

# *Introduzione*

> "Del resto non è difficile a vedersi come la nostra età sia un'età di gestazione e di trapasso a una nuova èra; lo spirito ha rotto i ponti col mondo del suo esserci e rappresentare, durato fino ad oggi; esso sta per calare tutto ciò nel passato e versa in un travagliato periodo di trasformazione"
>
> G.W.F. HEGEL

Il titolo del presente volume su "il diritto nell'età dell'informazione" necessita di un chiarimento iniziale. Mentre infatti, nel caso del diritto, il richiamo va a un termine oltremodo complesso ma familiare, la nozione d'informazione è solitamente intesa in chiave semantica, vale a dire come dati dotati di significato. Ma, appunto, in che senso l'indagine sul diritto è qui precisata dall'informazione come chiave di lettura per tracciare un periodo della storia umana?

Per rispondere a questa prima domanda, occorre passare al sottotitolo del libro su "il riposizionamento tecnologico degli ordinamenti giuridici". Il filo conduttore del volume è che siamo soltanto agli inizi di una radicale trasformazione che non soltanto interessa i sistemi giuridici contemporanei ma, altresì, gli attuali assetti politici, economici e sociali. La ragione dipende in buona sostanza da un particolare tipo di tecnologia che ingenera un inedito bisogno nelle odierne società. Si tratta di un vistoso cambiamento che viene reso, nel corso della trattazione, con la formula della "ICT-dipendenza". Di cosa si tratta?

Cominciamo dall'acronimo: come accennato fin dalla prefazione, "ICT" va riferito a quanto in inglese è riassunto come *Information and Communication Technology* e, in italiano, viene comunemente tradotto come tecnologia dell'informazione e della comunicazione. In questa occasione, come in altri casi, si è mantenuto la versione inglese dell'acronimo nel libro, vuoi perché è quella originaria, vuoi perché universalmente conosciuta nel campo dell'informatica e delle scienze sociali. Basti dire che a nessuno è ancora venuto in mente di redigere una voce "TIC" in Wikipedia. Nei casi in cui l'uso degli acronimi italiani sia invece invalso come moneta corrente del linguaggio quotidiano, ci si è semplicemente attenuti alla convenzione. Tra gli indici, il lettore troverà comunque una lista dei diversi acronimi impiegati, sia pure con la dovuta parsimonia, nel testo: ICANN, ITU, FMI, NSA, ONU, UE, WIPO, ecc.

Passando alla sostanza del discorso, la "ICT-dipendenza" sta a indicare un dato semplice, ma essenziale. Fin dall'inizio della storia, nel senso preciso del termine per cui la distinguiamo dalla preistoria, gli uomini hanno fatto uso di questo tipo di tec-

nologia, a partire dalla basica, la scrittura. È infatti questa rappresentazione convenzionale delle espressioni linguistiche che ha permesso agli uomini di trasmettere e conservare la memoria dei tempi andati. Sebbene rimanga controverso quando e dove collocare la nascita della scrittura, è significativo il rapporto ambiguo che un filosofo come Platone, a cavallo del quarto secolo a. C., intrattiene con ciò che egli definiva come "arte". Gli ammonimenti di Thamus nel dialogo *Fedro*, riportati nel capitolo primo, suggeriscono l'ambivalenza di chi, pur avendo scritto 36 opere mirabili, nutre pur sempre dubbi sull'uso di questa tecnologia.

Nel corso dei ventiquattro secoli che ci separano da Platone, emerge tuttavia un fatto cruciale. Nonostante le società umane abbiano certamente fatto uso della scrittura, esse, anche dopo l'invenzione della stampa a caratteri mobili nel quindicesimo secolo, hanno dovuto fare affidamento su altri tipi di tecnologia per provvedere alla propria sopravvivenza e sostentamento. Si pensi allo sviluppo dei metodi per lo sfruttamento di risorse basiche nel campo dell'agricoltura, nel settore tessile, o per le fonti di energia. È il caso dei mulini a vento e, poi, dei mulini ad acqua, diffusi dall'epoca romana, a cui si devono aggiungere i metodi per la combustione del legno. Soltanto in pieno medioevo, sarebbe stato affiancato al legno lo sfruttamento dell'energia fossile del carbone. Alla rivoluzione energetica occorsa tra sei e settecento, prima con l'invenzione della pentola a vapore e, poi, con le macchine di James Watt (1736-1819), avrebbe fatto séguito quella che viene comunemente definita come la prima rivoluzione industriale, tra i cui settori nevralgici ritroviamo come chiave di volta quello tessile.

Senza dover ricostruire in questa sede le intere gesta dell'uomo tecnologico, è sufficiente ricordare come qualcosa di altrettanto nuovo e rivoluzionario sia occorso a partire dalla seconda metà del secolo scorso con l'invenzione degli elaboratori elettronici e la progressiva convergenza delle tecnologie imperniate sul trattamento, la trasmissione, la ricezione ed elaborazione delle informazioni. Una molteplicità d'indicatori e formule sono state man mano proposte per compendiare il mutamento. Alle definizioni in negativo – quali la società post-industriale, post-fordista o post-moderna – hanno fatto da controcanto quelle positive della società, o l'economia, della conoscenza, la società in rete o, secondo la proposta adottata dall'Unione europea, la società dell'informazione. Qui, l'accento cade sulla ICT-dipendenza delle società odierne per rimarcare un aspetto specifico di questa trasformazione: se, nel corso di all'incirca quattromila anni, le società hanno fatto uso di ICT – ma sono rimaste fondamentalmente dipendenti dalle tecnologie volte allo sfruttamento delle fonti di energia e di altre risorse vitali – le società con cui siamo invece alle prese all'inizio del XXI secolo, dipendono tecnologicamente dall'informazione come proprio elemento essenziale.

Nel corso del primo capitolo avremo modo di dilungarci su quest'ultimo punto dell'indagine che, poi, rappresenta il nuovo scenario entro il quale collocare la presente disamina; ma, per intanto, provate a staccarvi dal vostro cellulare!

La tesi che andiamo a discutere è che siamo soltanto all'inizio di una rivoluzione epocale che, in quanto tale, non può che incidere sull'altro termine di riferimento del presente volume, il diritto. Lasciando per ora in sospeso il modo in cui s'intenda definire o concepire il fenomeno giuridico con le istanze tradizionali del giusnaturalismo, del giuspositivismo, dell'istituzionalismo, del costituzionalismo, del realismo, e via dicendo, l'idea di fondo è che si assista a un radicale riposizionamento del di-

ritto stesso. A scanso di equivoci, non si vuole suggerire con questo un rapporto unidirezionale, stante il quale la rivoluzione tecnologica apparirebbe come la causa di effetti in senso lato sociali, quasi che il diritto sia il mero effetto, o semplice spettatore passivo, dei processi in corso. Nel presentare a tempo debito il diritto come una specifica meta-tecnologia, avremo anzi occasione d'insistere sull'interazione e la tensione esistente tra i profili regolativi della tecnologia, il diritto e la società. In sintesi, se è evidente che il progresso tecnologico non possa che incidere sulle dinamiche degli ordinamenti giuridici – come occorso, ai suoi tempi, con l'invenzione della stampa e il suo impatto sul diritto scritto in occidente – è altrettanto innegabile che gli ordinamenti giuridici e sociali possono condizionare a loro volta i tempi e le forme del progresso tecnologico.

Per chiarire il significato di questa interazione tra tecnologia, diritto e società, il presente volume viene strutturato in due parti, ciascuna delle quali a sua volta suddivisa in cinque capitoli. Nella prima, l'attenzione sarà incentrata in termini generali sul riposizionamento tecnologico del diritto; nella seconda, si approfondirà questo quadro generale in rapporto a un settore specifico di questo riposizionamento, quello che attiene al diritto alla privacy e con il trattamento e la tutela dei dati personali.

*****

Nella prima parte del volume, l'intento è di mostrare cosa stia mutando, o sia già cambiato, rispetto alla tradizione giuridica, nell'era delle società ICT-dipendenti. Chiarita, nel primo capitolo, la portata dell'odierna rivoluzione tecnologica, il passo successivo dell'indagine consiste nel definire il senso del riposizionamento tecnologico del diritto. A tal fine, nel capitolo secondo, sono prese in considerazione tre diverse accezioni di complessità giuridica, ossia in termini d'informazione, d'emergenza di ordini spontanei e d'interdipendenza sistemica.

Non si tratta, con ogni evenienza, di concetti sconosciuti alla tradizione. Basti riferire che le accezioni di complessità cui si è fatto ora cenno, possono ricondursi rispettivamente al pensiero di Hobbes (l'informazione giuridica), alle opinioni degli antichi sui costumi, gli usi o le consuetudini (gli ordini spontanei), fino alla dottrina cosmopolitica di Kant (l'interdipendenza sistemica). Secondo uno dei motivi ricorrenti del presente volume, vedremo nondimeno come, nel mutare la scala o dimensione dei problemi, per via dell'accresciuta complessità dei fenomeni indagati, muti di conseguenza la forma in cui detti problemi vadano affrontati sul piano delle istituzioni, delle norme giuridiche e in senso strettamente operativo.

Nel capitolo terzo, l'attenzione sarà così incentrata sui profili istituzionali di questo mutamento, alla luce del passaggio che ha condotto dalle tradizionali forme di governo, che gli studenti affrontano nei corsi di diritto costituzionale del proprio paese, a quelle dell'odierna governance. In sostanza, il dato di fatto con il quale occorre fare i conti è che l'apparato degli stati nazionali sia stato più spesso affiancato, e in molti casi sostituito, da un complesso reticolo istituzionale, composto da attori, ora privati ora pubblici, sul piano internazionale e transnazionale, attraverso il quale le decisioni sono prese e l'autorità viene esercitata in un ordinamento determinato. Per illustrare sin d'ora i termini della questione, valgano due esempi: il primo concerne quell'intricato reticolo di attori istituzionali che compongono la governance

d'internet; il secondo riguarda ciò che, nelle parole della Corte di giustizia di Lussemburgo, rappresenta un "nuovo ordinamento nella storia del diritto internazionale", ossia la governance dell'odierna Unione europea.

Nel capitolo quarto, il fuoco dell'analisi verterà invece sui profili normativi del mutamento che si è, per così dire, cristallizzato nel sistema delle fonti e, cioè, dei fattori di produzione giuridica delle società ICT-dipendenti. Rispetto al modello invalso tra i moderni, a partire dalla pace di Westfalia (1648), il nuovo sistema appare più complesso perché, da un lato, aggiunge alla dicotomia tra diritto nazionale e diritto internazionale, la nuova dimensione del diritto transnazionale; e, d'altro canto, integra il vecchio dogma della legge come fonte per antonomasia del diritto con la giurisprudenza, i contratti e le norme sociali. Alla tradizionale configurazione delle fonti – "monista" sul fronte interno e "dualista" in chiave internazionale – subentra un sistema pluralista e spiccatamente policentrico che, ancora una volta, trova l'esempio più chiaro nella disciplina giuridica di internet. È quanto meno significativo che in uno dei suoi settori chiave, vale a dire il sistema dei nomi a dominio di primo livello e con la numerazione per il flusso dei dati in internet, le decisioni siano tuttora prese formalmente da una società privata con sede in California e che gli stati sovrani nazionali non dispongano al riguardo di alcun potere di veto.

Nel capitolo quinto, l'indagine avrà di mira uno degli aspetti più innovativi, ma anche altamente problematici, della rivoluzione in corso – cioè a dire gli ambiti e finalità del design – al fine di chiarire come le regole del diritto siano immesse più spesso negli ambienti, spazi e oggetti che mediano l'interazione dei soggetti. È il caso dei dispositivi a tutela della proprietà intellettuale nei sistemi elettronici, o dei sistemi di filtraggio in rete. Sebbene neanche in questo caso si tratti di un'idea del tutto nuova, come mostra l'impiego dei dossi stradali per far rispettare i limiti di velocità imposti dalla legge, si ha tuttavia a che fare ancora una volta con un effetto di scala. La ragione che, sempre più frequentemente, spinge a immettere le regole del diritto nel design delle cose, è infatti di affrontare i problemi posti dall'innovazione tecnologica, come nel caso dell'effettività della legge nello spazio transfrontaliero d'internet, per mezzo della tecnologia stessa. Alla canonica rappresentazione del diritto come mezzo di controllo sociale che si avvale della minaccia di sanzioni fisiche, subentra di qui la tentazione di attuare il diritto in forma automatica.

Alla luce di questo quadro generale sulle istituzioni, le norme e le questioni più strettamente tecniche del diritto nell'era delle società ICT-dipendenti, la parte speciale del volume è dunque incentrata su un settore specifico dell'ordinamento, ossia, quello della tutela del diritto alla privacy e con la protezione dei dati personali. Altri settori come il diritto penale, di guerra e di pace, il commercio elettronico o la proprietà intellettuale, avrebbero potuto dar conto del senso dell'odierno riposizionamento tecnologico del diritto. La scelta è tuttavia ricaduta su ciò che andremo man mano chiarendo nei termini della privacy informazionale, sulla base dei quattro ordini di considerazioni svolti nella seconda parte del libro.

*****

La prima ragione d'interesse per la privacy è introdotta nel capitolo sesto, dove l'accento è posto sulle leggi entrate in vigore all'indomani degli attacchi dell'11 set-

tembre 2001, con la cosiddetta "guerra al terrore" e il tradizionale fine degli stati di proteggere sia la sicurezza nazionale sia l'ordine pubblico. Nell'assumere il punto di vista della tutela alla privacy, siamo in grado di apprezzare come il fine degli stati di garantire l'ordine e la sicurezza sia mutato nel nuovo contesto tecnologico. Molto prima dello scandalo del programma Prisma dell'Agenzia di sicurezza nazionale americana (NSA), scoppiato nel 2013 a séguito delle rivelazioni di Edward Snowden, è indicativo che in molti abbiano evocato la "morte della privacy", stante l'arsenale dei mezzi tecnici messi a disposizione con la raccolta di metadati sulle comunicazioni elettroniche, sistemi di filtraggio o di geo-posizionamento satellitare (GPS), telecamere a circuito chiuso (CCTV), dati biometrici e ulteriori tracce e contenuti digitali disseminati con le email, acquisti tramite carte di credito e operazioni bancarie, prenotazioni di macchine o alberghi, il tutto poi raccolto e processato in gigantesche banche dati. Sebbene, come argomenteremo, la tesi della "morte della privacy" non è che una semplificazione giornalistica, essa ha avuto, e riscuote tuttora di, un grande successo, perché sintetizza il senso di spaesamento provocato dalla rivoluzione tecnologica in corso.

Dopo di che, la scelta di esaminare il riposizionamento tecnologico del diritto in rapporto alla tutela della privacy dipende dal fatto che, per via della dimensione globale dei problemi in gioco, bisogna mettere a confronto sistemi e ordinamenti diversi. Mentre, nel capitolo settimo, si esaminerà il modello statunitense di tutela con particolare riguardo alle decisioni della Corte suprema di Washington, nel capitolo ottavo sarà invece analizzato il quadro normativo vigente nell'Unione europea, prestando soprattutto attenzione alle direttive introdotte dai legislatori di Bruxelles. La peculiarità di ciascun sistema giuridico sul piano delle fonti sarà approfondita, ancora una volta, alla luce delle sfide poste dall'innovazione tecnologica. Nel caso americano, il riposizionamento verrà precisato dall'evoluzione giurisprudenziale della Corte in tema di privacy, a contatto con i problemi posti dall'uso delle intercettazioni telefoniche, dei sensori termici, dei satelliti e dal GPS; nel caso europeo, sempre l'innovazione tecnologica, ma questa volta sul fronte delle banche dati, spiega perché mai, fin dall'inizio degli anni settanta del secolo scorso, si sia cominciato opportunamente a distinguere dalla tradizionale tutela della privacy, una nuova e autonoma sfera di tutela e, cioè, quella relativa ai dati personali.

La terza ragione d'interesse per questi temi dipende dall'accennata sensibilità tecnologica dei diritti alla privacy e alla tutela dei dati; ma, questa volta, dal punto di vista del rapporto che li lega ai restanti diritti e libertà tutelati dall'ordinamento. Secondo quest'ulteriore prospettiva, introdotta nel capitolo nono, la tutela della privacy e la protezione dei dati personali si profilano non solo come punto di snodo per settori cruciali del diritto, come la sicurezza nazionale o l'ordine pubblico, ma anche riguardo alla libertà di parola e di pensiero, al diritto di cronaca e all'informazione, al riuso delle informazioni del settore pubblico e con la tutela della proprietà intellettuale, fino alla tradizionale protezione relativa alla riservatezza e all'identità personale, contro gli atti diffamatori, la diffusione dei fatti privati o la loro distorsione sotto falsa luce. Il fatto che il diritto alla privacy e la tutela dei dati personali appaiano come una sorta d'interfaccia tra il fine della sicurezza nazionale e i restanti diritti e libertà protetti dall'ordinamento, solleva però un paradosso che rappresenta

il quarto, e ultimo, motivo d'interesse per la materia. Il paradosso riconduce alle considerazioni generali sul riposizionamento del diritto da cui abbiamo preso le mosse in questa introduzione.

*****

Abbiamo accennato precedentemente al fatto che, sul piano delle fonti, la legge non rappresenti più il fattore produttivo unico del sistema giuridico, secondo i dettami del monismo invalso tra i moderni con il cosiddetto "modello di Westfalia". Alle norme del legislatore nazionale bisogna infatti affiancare il ruolo svolto dalla giurisprudenza, i contratti, specie nel diritto transnazionale, e le norme sociali. Per giustificare la tesi, basti ancora una volta un esempio, sia pure paradigmatico, sul modo in cui larga parte dell'interazione sociale in rete sia legata alla possibilità di scelta tra ordinamenti diversi. Questa scelta, che prima dell'era d'internet era appannaggio per lo più esclusivo delle imprese multinazionali, si è per così dire democratizzata, nel senso che si è estesa a raggiera tra gli utenti della rete che, spesso, preferiscono seguire le consuetudini e usi invalsi nel nuovo ambiente digitale, piuttosto che le norme stabilite da un legislatore percepito come distante e, a volte, perfino in mala fede o ignorante. Quando, poi, le norme del rapporto sono stabilite dalle condizioni di servizio imposte dalle imprese, come avviene quotidianamente con Facebook, Google, Apple, eBay, Netflix, e via dicendo, coloro che sono sottomessi all'autorità di quelle regole lo fanno ancora una volta sulla base delle loro scelte, secondo un meccanismo che, con formula inglese, viene riassunto come "opt in", piuttosto che "opt out" (come avviene invece con gli stati). Il risultato non è certo una sorta di paradiso terrestre; ma, nell'eventualità di controversie, capiremmo ben poco di come funzionino gli ordinamenti giuridici contemporanei se non prestassimo attenzione a cosa succede nel caso di un complesso sistema normativo transnazionale come quello di eBay. La maggior parte delle liti non finisce davanti alle corti degli stati nazionali, sia per via del valore economico esiguo delle dispute, che sconsiglia il più delle volte il ricorso a quelle corti, sia per la natura delle controversie che hanno a che fare con individui che talora risiedono in altre parti del pianeta, sia per l'efficienza del sistema legale di eBay che deve, pur sempre, mantenere la fiducia dei propri utenti, se vuole continuare a fare affari.

A prevenire anche in questo caso equivoci, come già, in termini generali, a proposito del rapporto tra i profili regolativi della tecnologia, il diritto e la società, occorre avvertire che le precedenti annotazioni non intendono certo suggerire che le nuove forme degli ordinamenti giuridici nell'era delle società ICT-dipendenti finiscano per dover aggiungere alla lista dei disoccupati sia i legislatori che le corti nazionali. Alla fitta rete di leggi e di accordi internazionali che hanno caratterizzato la cosiddetta "guerra al terrore", cui si è fatto prima cenno, è il caso di aggiungere sin d'ora le disavventure giudiziarie di una società come Google e come, nel travaglio di un nuovo regolamento per la tutela dei dati personali in Europa (2012-2014), i legislatori di Bruxelles siano venuti minacciando multe salate per tutte le società che non provvedano a rispettare i nuovi obblighi previsti dalla normativa.

Assodato, pertanto, che il riposizionamento tecnologico del diritto non implica affatto un diritto senza legislatore, bisogna però far caso al significato di questo stes-

so riposizionamento che, poi, riconduce al paradosso sotteso al quarto e ultimo motivo d'interesse per i temi della privacy e la tutela dei dati personali. Nell'accingerci a studiare la pletora di leggi, nazionali e internazionali, che mirano a disciplinare questo settore dell'ordinamento, occorre infatti considerare come le leggi non operino per lo più in una sorta di vuoto normativo; ma siano, bensì, da ricondurre alle convenzioni e pratiche sociali tese a risolvere il problema del coordinamento morale tra i consociati. Più che dalla legge, in altri termini, il luogo normativo dell'autorità politica è rappresentato dalle convenzioni o pratiche sociali a cui la legge trasmette la propria autorità. Avendo a mente l'opera di bilanciamento resa necessaria nel caso della privacy, tra le ricordate esigenze di sicurezza nazionale e ordine pubblico da un lato e, dall'altro, la tutela degli ulteriori diritti e libertà dell'ordinamento, il paradosso è che, spesso, tanto i destinatari delle norme dei legislatori quanto gli stessi esperti finiscono per trovarsi in gravi difficoltà, allorquando devono orientarsi nella giungla di leggi, precedenti delle corti e raccomandazioni delle autorità indipendenti, su come tracciare la linea di confine tra lecito e illecito.

Nel modello statunitense di tutela della privacy, è rimarchevole come il nesso che viene in questo modo a instaurarsi tra i comandi del legislatore e i destinatari delle norme sia mediato dalla dottrina che la Corte suprema di Washington ha messo a punto fin dal 1967, sulla base di un test che, per via del caso da cui ha tratto origine, è noto come "test di Katz". L'idea di fondo è che ogni individuo abbia diritto a vedere tutelata la propria aspettativa di privacy nei confronti del governo – se del caso, dichiarando l'illegittimità costituzionale delle norme approvate dal legislatore federale – a condizione che la società sia pronta a riconoscere tale aspettativa soggettiva di tutela come "ragionevole". Sebbene non siano mancati i problemi inerenti alla applicazione del test nel corso di quasi mezzo secolo, esso ha avuto il merito di proporre un ponte tra il luogo normativo dell'autorità politica e le sue leggi; che è, poi, la ragione principale per cui, nell'ultimo capitolo del libro, si è provveduto a una nuova forma di "trapianto giuridico". Davanti alla fitta rete di disposizioni normative che hanno reso difficile orientarsi, nel vecchio continente, a proposito di quali siano i propri diritti in un settore così cruciale dell'ordinamento, l'idea è di testare le norme del legislatore di Bruxelles, alla luce di un criterio maturato sia pure in una cultura e in un ordinamento, per molti versi, assai diverso da quello europeo.

C'è però un ulteriore motivo che consiglia di ammettere il test sulla ragionevole aspettativa di privacy in Europa. La ragione riconduce al punto dal quale siamo partiti, la rivoluzione tecnologica; e al ritmo, per certi aspetti vertiginoso, del suo andamento, che rischia di rendere l'intervento del legislatore perennemente in ritardo, oppure di essere frequentemente rivisto per via dello stesso sviluppo tecnologico. All'oscurità dei testi di legge che dovrebbero, viceversa, orientare gli individui, va infatti aggiunto il senso di spaesamento prodotto dall'incalzare della rivoluzione in corso, sia per quanto attiene alle aspettative dei cittadini, sia in rapporto alle decisioni politiche che le autorità devono assumere. Alla pletora di liti giudiziarie che esamineremo in questo volume per via dei problemi regolativi che la tecnologia ha posto con l'uso del telefono e le cabine telefoniche, le camere fotografiche per gli aerei e i satelliti, i sensori termici e il GPS, i metodi per l'identificazione biometrica e gli strumenti d'analisi come il *data mining* e la profilazione, la rivoluzione tecnolo-

gica è pronta a proporre ulteriori sfide con una nuova generazione di agenti artificiali autonomi e oggetti che comunicano tra di loro in ambienti intelligenti. Tenuto conto del rapporto che lega le convenzioni sociali al piano normativo dell'autorità politica, alcune decisioni di quest'ultima suggeriscono come sia forse il caso di fare fin d'ora i conti con un "test di Katz" europeo.

# Parte Generale

## *Il riposizionamento tecnologico del diritto*

# I.
# *Tecnologia*

> "La tecnologia consiste nella produzione del superfluo – oggi come nell'era paleolitica. Questa è la ragione per cui gli animali sono atecnici; essi si accontentano del semplice atto di vivere"
>
> José ORTEGA Y GASSET

Possiamo iniziare la nostra indagine sul diritto nell'era delle società ICT-dipendenti, muovendo dalla parte iniziale di un noto film, *2001 Odissea nello spazio*, in cui due gruppi di ominidi vengono a confronto per stabilire a chi spetti un dato territorio. Lo scontro ha termine quando uno dei contendenti, avvalendosi di un femore trovato lì per caso, lo impiega come arma letale per far fuori l'avversario. In uno degli "stacchi" più noti nella storia del cinema, l'immagine dell'osso-arma lanciato in aria dall'ominide vittorioso lascia improvvisamente spazio a quella di una navicella spaziale. Come informa la relativa voce del film in Wikipedia, secondo il regista Stanley Kubrick "ognuno è libero di speculare a suo gusto sul significato filosofico del film, io ho tentato di rappresentare un'esperienza visiva, che aggiri la comprensione per penetrare con il suo contenuto emotivo direttamente nell'inconscio". Sebbene ciascuno di noi sia dunque autorizzato a speculare a proprio piacimento sul significato del film – a partire dallo stacco che dagli ominidi in lotta nell'Africa di quattro milioni d'anni or sono conduce alle forme di intelligenza artificiale presenti nella navicella spaziale in viaggio verso Giove – sembra lecito interpretare l'esperienza visiva del film all'insegna della chiave di lettura offerta dalla tecnica. Lo "stacco di Kubrick" fa da ponte tra l'alba dell'uomo tecnologico e gli sviluppi odierni del nostro saper fare (*know how*).

Passando dalla critica cinematografica all'indagine filosofica, l'interpretazione in chiave tecnica dello stacco di Kubrick richiede nondimeno di essere approfondita sulla base di due ulteriori riflessioni, chiamiamole (R1) e (R2), e di un plesso di problemi (P).

(R1): pare incontestabile che, al fine di garantirsi la sopravvivenza sul pianeta e venire a capo delle sfide per l'adattamento all'ambiente, l'uomo, nel corso di centinaia di migliaia di anni, abbia dovuto affidarsi al proprio talento tecnologico, e cioè alla propria capacità tecnica di "saper fare". Non essendo stato dotato di un particolare equipaggiamento fisico, quanto a vista, udito o forza muscolare, si è trattato in fondo di una scelta obbligata che, a sua volta, ha finito per retroagire sul corredo genetico e sullo stesso ambiente in cui l'*homo technologicus* si ritrova a vivere.

(R2): soddisfatta l'esigenza primaria della sopravvivenza, il saper fare dell'*homo technologicus* si è progressivamente esteso a nuove sfide. Ad esempio, nella ricostruzione che il grande filosofo greco Platone (428-427 – 348-347 a. C.) compie nel secondo libro de *La Repubblica*, questo snodo evolutivo è interpretato con il passaggio dalla "città primitiva" alla "città opulenta", secondo una lettura che tornerà nell'opera di un filosofo spagnolo, José Ortega y Gasset (1883-1955), come riassunto nell'epigrafe di questo capitolo.

(P): qual è mai il rapporto tra (R1) e (R2)? Tornando allo stacco di Kubrick, dobbiamo forse cogliere il passaggio dalla scoperta della tecnica da parte degli ominidi africani alle forme di intelligenza artificiale delle navicelle spaziali in viaggio verso Giove, come un passaggio in qualche modo necessario, come suggeriscono coloro che, in queste pagine, sono indicati come gli esponenti del tecno-determinismo? O, come propongono gli studiosi delle scienze della complessità e della teoria del caos, questo passaggio non era affatto necessario, perché sensibile a troppe variabili e condizionamenti? Inoltre, ammessa e non concessa l'inevitabilità del passaggio da (R1) a (R2), lo dobbiamo cogliere in termini di "progresso" oppure scellerata spensieratezza? E che ne è del diritto in questo contesto? Quale il suo ruolo in rapporto alle sorti dell'*homo technologicus*?

Al fine di venire a capo di questi interrogativi e offrire l'impianto generale del presente volume, l'indagine di questo capitolo è suddivisa in quattro parti. In primo luogo (§ 1.1), l'attenzione andrà rivolta al pensiero di Aristotele e al modo in cui egli ha inteso formalizzare la relazione tra (R1) e (R2) come rapporto tra diverse forme di sapere, vale a dire teoretico, pratico e tecnico. Questa prospettiva consente di chiarire quale tipo di sapere spetti al diritto e, sulla base di una digressione metodologica, quale sia il livello di astrazione secondo cui il sapere giuridico è inteso in questo libro, e cioè il punto di vista che assume il diritto come una meta-tecnologia.

Nel § 1.2, ci si concentrerà sulla tesi per molti versi opposta a quella del diritto come meta-tecnologia, ossia quella dei fautori del tecno-determinismo: sulla scorta di alcuni contro-esempi, l'intento è non solo di mostrare come il progresso tecnologico non sia predeterminato o necessitato ma, per ciò stesso, come lo scopo del diritto di regolare il progresso tecnologico non sia il semplice frutto della vanagloria dei giuristi. In fondo, se avessero davvero ragione i tecno-deterministi, il libro troverebbe qui la propria conclusione!

Nel § 1.3, l'argomentazione ruoterà attorno a uno dei cavalli di battaglia del tecno-determinismo, riassumibile con la "legge di Moore": in fondo, è un dato di fatto che la potenza di calcolo degli elaboratori elettronici sia raddoppiata ogni diciotto mesi nel corso degli ultimi cinquant'anni, mentre le capacità ottiche sono duplicate ogni anno e quelle della tecnologia senza fili, al pari del numero di robot commerciali e militari, ogni nove mesi. La tesi è che si debba fare i conti con la stupefacente accelerazione del progresso tecnologico senza, per questo, sposare il più delle tesi tecno-deterministe.

Infine, nel § 1.4, l'accento cadrà su un aspetto cruciale della rivoluzione tecnologica: per la prima volta nella storia dell'umanità, le odierne organizzazioni sociali dipendono dall'uso delle tecnologie dell'informazione e comunicazione (ICT), come proprie risorse vitali. Questo cambiamento non può che investire radicalmente la sfera giuridica: si tratta dei temi e motivi dell'aumento della complessità sociale che saranno l'oggetto del capitolo secondo.

## 1.1. *I saperi dell'*homo technologicus

Si è fatto cenno alla distinzione tra l'impiego della tecnica per il soddisfacimento delle esigenze basilari dell'uomo, quali la propria sopravvivenza sul pianeta, e l'uso della tecnica per la produzione di beni superflui nella "società opulenta" di Platone. La distinzione viene fatta dal filosofo per bocca di Socrate (470-469 – 399 a. C.), nel secondo libro de *La Repubblica*, nel dialogo con il fratello maggiore di Platone, Glaucone, al fine di "costruire a parole uno stato fin dalla sua origine" [1].

Da un lato, a detta di Socrate, "uno stato nasce perché ciascuno di noi non basta a se stesso, ma ha molti bisogni […] Così, per un certo bisogno ci si vale dell'aiuto di uno, per un altro di quello di un altro: il gran numero di questi bisogni fa riunire in un'unica sede molte persone che si associano per darsi aiuto, e a questa coabitazione abbiamo dato il nome di stato [*polis*]" (369b5-c5). All'origine delle comunità umane, quindi, troviamo un criterio utilitaristico, fondato sulla divisione del lavoro, per cui "il nucleo essenziale dello stato" consta all'inizio di "quattro o cinque persone", ciascuna delle quali dovrà saper fare, evidentemente, il proprio lavoro. Dal "primo e maggiore bisogno [che] è quello di provvedersi il nutrimento per sussistere e vivere", i personaggi che con la loro tecnica danno vita alla città sono, oltre all'agricoltore, il muratore, il tessitore e il calzolaio, che a loro volta avranno bisogno degli attrezzi per svolgere il proprio lavoro: "ecco dunque che carpentieri, fabbri e molti altri simili artigiani verranno a far parte del nostro staterello e lo renderanno popoloso [e] non sarebbe ancora troppo grande se vi aggiungessimo bovai, pecorai e le altre categorie di pastori" (370d3-e1, p. 78).

D'altro canto, soddisfatti i bisogni elementari dell'uomo e innanzi alla prospettiva di una vita frugale, spesa tutto il giorno a lavorare duramente sui campi, spetta a Glaucone farsi carico di esprimere i bisogni della società opulenta, alla quale corrispondono di necessità nuove figure sociali. Al saper fare di agricoltori e muratori, di tessitori e calzolai, dovranno di qui aggiungersi imitatori e valletti, rapsodi e attori, coreuti e impresari, stilisti e servi, pedagoghi, balie e nutrici, acconciatrici, barbieri e cuochi. "Bene, risposi [Socrate], comprendo. A quanto sembra, non vogliamo soltanto sapere come nasce uno stato, ma uno stato gonfio di lusso. Forse però non è un male, perché così vedremo probabilmente come nascono negli stati giustizia e ingiustizia" (372d6-e6, p. 80). Infatti, a giudizio di Socrate, la nascita della società opulenta o, se si preferisce, la fine di quella primitiva, comporta inevitabilmente il sorgere del conflitto tra gli uomini, poiché il territorio fin lì sufficiente a nutrire i suoi abitanti, diventerà piccolo e porterà a "prenderci una porzione del territorio dei vicini se vorremo aver terra sufficiente per pascolare e arare" (373d4-e1, p. 81). La conseguenza è che ci sarà bisogno non soltanto di una nuova classe sociale, vale a dire l'esercito con la tecnica dei guerrieri; ma la necessità di saper ora difendersi, ora aggredire, conduce al classico problema di chi debba mai custodire i custodi. "La verità è questa: lo stato in cui chi deve governare non ne ha il minimo desiderio, è per forza amministrato benissimo, senza la più piccola discordia […] Se invece

[1] Riprendendo la tr. it. di Franco Sartori (PLATONE, *La Repubblica*, ed. Laterza, Roma-Bari 2000), i rinvii bibliografici nel testo sono quelli tradizionali: nel caso, il rimando è a 369 c 8-9, p. 77.

vanno al potere dei pezzenti, avidi di beni personali e convinti di dover ricavare il loro bene di lì, dal governo, non è possibile una buona amministrazione: perché il governo è oggetto di contesa e una simile guerra civile e intestina rovina con loro tutto il resto dello stato" (520d1-521a10, pp. 235-236).

Possiamo qui interrompere il racconto platonico, al fine di sottolineare come al saper fare delle "quattro o cinque persone" con cui ha avuto inizio la città, subentri, con la politica, un nuovo tipo di sapere. Dal punto di vista di Platone, si tratta di un sapere che appare necessariamente più alto e più nobile, rispetto al saper fare dei ceti produttivi: è l'intelligenza politica dei filosofi-re. Questa distinzione è sostanzialmente mantenuta dal grande allievo di Platone, Aristotele (384-322 a. C.), nel primo libro della *Metafisica*, in cui si legge che, prima, dovettero costituirsi le arti dirette al soddisfacimento dei bisogni vitali e, dopo, "quando già si erano costituite tutte le arti di questo tipo [rivolte all'utile], si passò alla scoperta di quelle scienze che non sono dirette né al piacere né alle necessità della vita, e ciò avvenne dapprima in quei luoghi in cui gli uomini dapprima furono liberi da occupazioni pratiche. Per questo le arti matematiche si costituirono per la prima volta in Egitto: infatti, là era concessa questa libertà alla casta dei sacerdoti" [2]. La sostanziale differenza tra Platone e Aristotele, pertanto, non consiste nell'ammettere la precedenza cronologica del sapere tecnico su quello scientifico e, dal punto di vista valoriale, la superiorità di quest'ultimo sapere su quello tecnico. Piuttosto, la differenza consiste nell'ulteriore distinzione che Aristotele delinea tra sapienza e saggezza, tra sapere teoretico e sapere pratico. "Ed è per questo che, come si è detto sopra, chi ha esperienza è ritenuto più sapiente di chi possiede soltanto una qualunque conoscenza sensibile: chi ha l'arte più di chi ha esperienza, chi dirige più del manovale e le scienze teoretiche più delle pratiche" (*Met.* 981b30-982a2, p. 7). La figura 1, qui sotto, illustra ciò che un noto storico della filosofia ha convenientemente riassunto come "le ragioni di Aristotele" (Berti 1989).

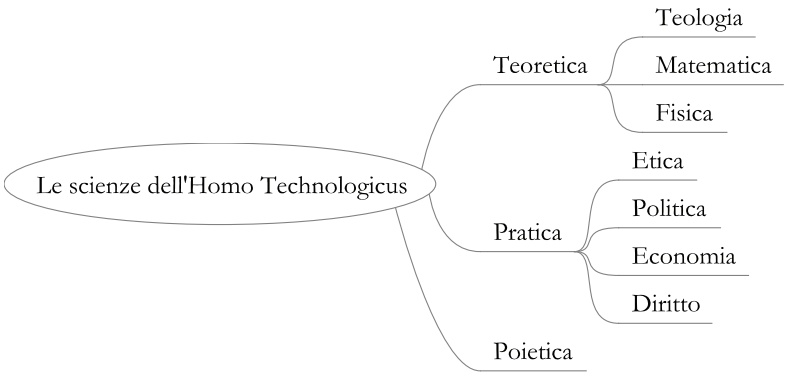


Figura 1: *Tra teoria e prassi*

[2] Sulla scorta della tr. it. di Giovanni Reale (ARISTOTELE, *Metafisica*, ed. Bompiani, Milano 2000), ancora una volta i rinvii bibliografici nel testo sono quelli tradizionali: in questo caso, il rimando è ARISTOTELE, *Met.* A 1, 981b20-25, p. 7.

Ad onor del vero, la novità che Aristotele introduce rispetto a Platone, nel distinguere tra sapere teoretico e pratico, poco cambia rispetto al modo in cui è stato tradizionalmente concepito dagli antichi il saper fare dell'uomo tecnologico. Si tratta di una conoscenza sostanzialmente subordinata ai parametri epistemici e valoriali messi a punto dai filosofi, per cui il risultato è che, al pari della speculazione di Platone, nemmeno quella aristotelica aiuterebbe in molto a capire l'impatto della tecnica sul diritto. Non è certo questa la tradizione filosofica cui rivolgersi per avere chiarimenti in merito! Tuttavia, soffermiamo l'attenzione sulla tripartizione aristotelica di teoretica, pratica e poietica, perché essa aiuta a chiarire preliminarmente l'oggetto di questo impatto, e cioè, appunto, il diritto stesso.

Di qui, ci concentreremo a continuazione sul significato della tripartizione aristotelica, al fine di cominciare ad avere dimestichezza con i termini della figura 1 (v. § 1.1.1). Dopo di che (§ 1.1.2), occorrerà una breve digressione metodologica sul "livello di astrazione" che intendiamo assumere rispetto ai termini della figura, vale a dire, il diritto come meta-tecnologia (§ 1.1.3). Su queste basi, potremo tornare al problema di quale impatto mai la tecnologia possa avere sul diritto, pace Platone e Aristotele, a detta degli esponenti del tecno-determinismo (§ 1.2).

### 1.1.1. *Teoresi, prassi e poiesi*

La distinzione che Aristotele coglie tra teoretica, pratica e poietica, ha a che fare tanto con la differenza d'oggetto di studio quanto con la finalità del sapere. Seguendo l'ordine cronologico messo in rilievo nel paragrafo precedente, si può dire che, per quanto concerne la razionalità poietica, essa consista nel saper fare, o produrre, qualcosa, sia ai fini essenziali, o del soddisfacimento dei bisogni vitali, della società primitiva, sia ai fini superflui o del lusso della società opulenta. Nel caso della ragion pratica, essa ha come oggetto le azioni umane e, più in particolare, secondo l'espressione dell'*Etica Nicomachea*, "le azioni belle e giuste" (*op. cit.*, 1094b11): si tratta di un sapere che non è fine a sé ma, bensì, un sapere per fare, come mezzo per l'azione. Infine, quanto alle scienze teoretiche, esse hanno come oggetto la matematica, la fisica e la teologia, per cui il fine è il sapere per il sapere, la verità fine a se stessa. Con le parole del filosofo, "è anche giusto denominare la filosofia scienza della verità, perché il fine della scienza teoretica è la verità, mentre il fine della pratica è l'azione. (Infatti, coloro che hanno per fine l'azione, anche se osservano come stanno le cose, non tendono alla conoscenza di ciò che è eterno ma solo di ciò che è relativo ad una determinata circostanza e in un determinato momento)" (*Met*. II, 993b24-26).

Naturalmente, per quanto concerne le scienze teoretiche, a detta di Aristotele, bisognerebbe distinguere ulteriormente tra il rigore dimostrativo della matematica, basato sul metodo apodittico, e il metodo dialettico della fisica (e della metafisica). Senza fare per questo di Aristotele un precursore del probabilismo moderno, le prove della fisica, al contrario della matematica, suggeriscono un parallelismo metodologico tra fisica e scienze pratiche, dato che le dimostrazioni della fisica, al contrario della matematica, valgono "per lo più" e non "sempre". A giudizio di Aristotele, qui in diretta polemica con Platone, "è proprio dell'uomo colto, infatti, richiedere in ciascun campo tanta precisione quanta ne permette la natura dell'oggetto,

giacché è manifesto che sarebbe pressappoco la stessa cosa accettare che un matematico faccia dei ragionamenti solo probabili e richiedere dimostrazioni da un oratore" (Aristotele ed. 2000: 53).

Lo stesso accorgimento metodologico, nondimeno, vale anche per lo studio delle azioni umane, in quanto, come attesta il caso dell'etica e della politica, la filosofia pratica, o scienza politica, è pur sempre una scienza. Bisogna per ciò distinguere la capacità di cogliere i principi della scienza nella particolarità dell'esperienza, dalla capacità di dimostrare ciò che è per lo più nelle faccende umane: una cosa, infatti, è la saggezza dell'uomo politico, ben esemplificata dalla *phrónesis* di Pericle, per cui l'intuizione gioca un ruolo determinante per sapere individuare ciò che è opportuno in determinate situazioni e, soprattutto, al fine di scegliere i mezzi attraverso i quali raggiungere i fini della buona politica. Altra cosa, però, è l'indagine della scienza politica vera e propria, o *epistème*, illustrata dall'insegnamento di Socrate, che si avvale della dialettica come metodo dimostrativo per la confutazione delle tesi tra loro contrapposte e assunte all'interno della totalità delle opinioni possibili (Aristotele ed. 2000: 237 e 251). Da quest'ultimo punto di vista, ne consegue che le rigide distinzioni dei saperi, come tratteggiate sopra nella figura 1, vanno in realtà relativizzate sia "verso l'alto", sia "verso il basso".

Verso l'alto perché, nonostante la differenza d'oggetto – il mondo della necessità nel caso delle scienze teoretiche, il mondo della libertà nel caso delle scienze pratiche – le virtù dianoetiche del sapere epistemico, o scientifico, accomunano il sapere pratico a quello teoretico. Questo è un punto su cui, tra i tanti, ha insistito con particolare rigore il filosofo tedesco Hans-Georg Gadamer (1900-2002), quando sottolinea le "implicazioni ontologiche" della filosofia pratica aristotelica, specie per quanto riguarda il suo punto di orientamento ultimo, "il modello dell'imperituro". Sebbene la distinzione che Aristotele delinea tra teoresi e pratica sia "manifestamente la conseguenza della sua critica dell'idea platonica di bene […] Aristotele può ripetere autentiche formulazioni platoniche quando cerca di descrivere la conformazione dell'uomo al Divino. Di lui non si può dire quello che Hegel ha preteso per se stesso", e cioè di superare l'aspirazione al sapere, o filo-sofia, nella sapienza stessa (Gadamer 1984: 257 e 260).

D'altra parte, la separazione dei saperi è relativizzata anche verso il basso, e cioè per quanto attiene al mondo della libertà, per un duplice ordine di motivi. Il primo riguarda le evidenti affinità tra la *phrónesis*, o saggezza, dello statista e l'*epistème*, o scienza, del filosofo, sia per la compenetrazione delle istanze pratiche e conoscitive nell'ambito della politica, sia perché in entrambi i casi è richiesta una certa esperienza di vita al politico e al filosofo. In secondo luogo, malgrado la differenza d'oggetto tra il mondo morale di cui si occupano i filosofi, e la sfera delle arti e della produzione, tanto le scienze pratiche quanto le scienze poietiche sono per l'appunto scienze relative al mondo della libertà. Inoltre, secondo l'annotazione della *Metafisica* (981b24-25), basti pensare che nessun uomo potrebbe aspirare a diventare saggio in uno stato corrotto: anzi, chi si occupa di politica e di etica non è mai disinteressato poiché, per dirla con il filosofo francese Eric Weil (1904-1977), "colui che parla di morale non fa un corso teorico, ma si sforza di rendere migliori i suoi concittadini" (Weil 1990: 38).

Sulla base di questa duplice "apertura" della filosofia pratica, possiamo tornare

al problema sollevato all'inizio di questo capitolo, e chiederci: quale, dunque, il ruolo del diritto? Quale il rapporto tra le istanze teoretiche, pratiche e tecniche della sfera giuridica? Più in particolar modo, quale il nesso tra i profili tecnici del diritto e le sfide poste dall'ambito della produzione sociale? Avendo a che fare con il fine di disciplinare tali sfide che provengono, per così dire, dal basso dell'esperienza, e tenendo del pari presente l'apertura verso l'alto delle istanze metafisiche, dobbiamo forse concludere che il diritto sia veramente una meta-tecnica, o una meta-fisica?

### 1.1.2. *Livelli di astrazione*

Dai tempi di Platone e Aristotele, i filosofi discutono e si dividono sia sul concetto del diritto, sia sui fini e modi in cui esso debba essere convenientemente rappresentato. Sul fronte del concetto, per esempio, ci sono gli esponenti del positivismo giuridico che, in estrema sintesi, ritengono che diritto sia soltanto quello posto in essere dagli organi dell'autorità costituita in un dato territorio; vale a dire, in era moderna, lo stato sovrano nazionale. A questi si contrappongono i sostenitori, antichi e moderni, della scuola del diritto naturale che ritengono vi sia un parametro di razionalità, dato dalle leggi o diritto di natura, sulla cui base giudicare della legittimità del diritto positivo. Poi, ci sono i teorici del realismo che insistono sui rapporti di forza, politici o economici, all'interno della società, come anche i teorici dell'istituzionalismo che fanno leva sulla continuità e peculiarità storica delle organizzazioni sociali, e via dicendo.

Sul fronte dei fini, le cose non vanno tanto meglio: a chi, come spesso accade con i teorici del giusnaturalismo, ritiene che il diritto sia uno strumento di comunicazione tra i soggetti, vanno contrapposti coloro i quali vedono nel diritto un mezzo di controllo sociale. Non mancano quindi i sostenitori della tesi intermedia, che assume il diritto sia come un medium della comunicazione intersoggettiva, sia come una tecnica del controllo sociale, magari specificando quest'ultimo scopo, ora con il fine di fare coesistere gli arbitri degli individui, ora con quello di far prevalere gli interessi di una classe sociale o, più semplicemente, come voleva il sofista Trasimaco nel ricordato dialogo platonico su *La Repubblica*, l'"utile del più forte".

Il lettore (e lo studente) non disperi: non è mia intenzione aggiungere alla lunga lista, una nuova versione di ciò che il diritto è o come esso debba essere, magari sulla scorta delle indicazioni aristoteliche riportate in precedenza. Piuttosto, l'intento è di individuare il livello di analisi adeguato a cogliere il rapporto tra fenomeno giuridico e progresso tecnologico.

Una breve digressione metodologica s'impone a questo punto della trattazione, per cogliere le ragioni di una prospettiva, quella del diritto come meta-tecnologia, che sarà resa esplicita nel prossimo paragrafo. In particolare, vale la pena di soffermarsi sulle riflessioni che Luciano Floridi, dal 2013 professore di filosofia ed etica dell'informazione all'Università di Oxford, ha svolto proprio su questa collana, *Digitalica*, a proposito "del metodo dei livelli di astrazione" o LdA (Floridi 2009). In sostanza, occorre scegliere il punto di vista, dal quale s'intende descrivere, esaminare e sottoporre le proprie argomentazioni attorno a un dato oggetto di studio. Prima ancora del concetto e fini del diritto, si pensi, ad esempio, al caso in cui si abbia a che fare con uno dei robot domestici che illustreremo nel capitolo nono (v. § 9.4.2).

Nel caso in cui, sfortunatamente, l'applicazione presenti qualche problema di funzionamento, è probabile che l'attenzione vada rivolta ora alle proprietà fisiche dell'artefatto, ora al suo design, poiché è ragionevole assumere che il robot sia stato prodotto al fine di compiere determinate operazioni e, dunque, si comporti conseguentemente. Trattandosi più spesso di "macchine intelligenti", e cioè di macchine in grado di apprendere dagli stimoli provenienti dall'ambiente che li circonda e dalla propria esperienza, è tuttavia probabile che in più occasioni entreranno in gioco le credenze e i desideri di un agente artificiale che si comporta al fine di raggiungere un determinato obiettivo (si v. Dennett 1987: 17). A seconda, perciò, del motivo per cui abbiamo a che fare con il robot domestico – ma, se per questo, con un animale o un essere umano – muta il plesso di proprietà, caratteristiche o peculiarità che saranno ritenute rilevanti.

Formalizzando, il livello di astrazione prescelto può dunque essere inteso come l'interfaccia che rende possibile l'analisi del sistema, mediante l'individuazione dei suoi "osservabili", vale a dire le proprietà, caratteristiche o peculiarità rilevanti a quel dato livello di astrazione. Naturalmente, tali osservabili potranno essere ulteriormente raffinati tramite le "variabili". Il risultato consiste in un modello per quel determinato settore: la figura 2 illustra questa metodologia.

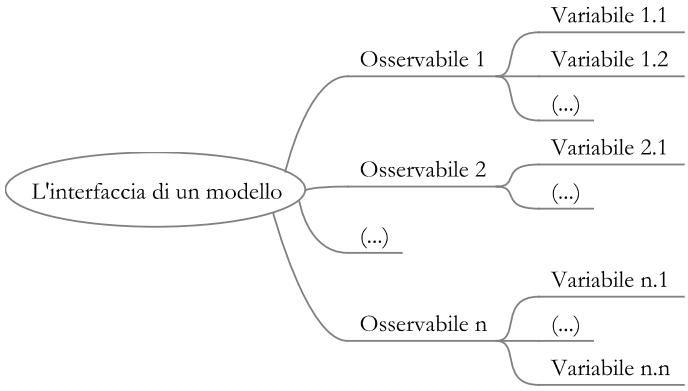


Figura 2: *Livelli d'astrazione*

Si tratta ora di comprendere come operi questo metodo nel campo del diritto e, in particolare, al livello definito dal diritto come meta-tecnologia.

### 1.1.3. *Il diritto come meta-tecnologia*

Si è fatto cenno nel paragrafo precedente, al fatto che non siano mancate le interpretazioni del diritto che lo intendono, ora, come tecnica volta a perseguire il fine della coesistenza degli arbitri individuali, ora, quello del controllo sociale. La prima chiave di lettura la si deve al filosofo tedesco Immanuel Kant (1724-1804); la seconda al giurista viennese e teorico neo-kantiano Hans Kelsen (1881-1973). Particolare rilevanza assume, in entrambi i casi, il ruolo della sanzione o momento coattivo del diritto. Nel caso del giusnaturalismo kantiano, la sanzione chiarisce il passaggio dal

diritto privato dello stato di natura al diritto pubblico dello stato civile, rendendo perentorio lo stato giuridico provvisorio delle regole presenti in natura. Nel caso del giuspositivismo kelseniano, invece, la sanzione distingue il diritto da altre forme di ordinamento sociale, secondo la formula "se A, allora B". Nella prospettiva della *Teoria generale del diritto e dello stato* (Kelsen 1959), il diritto è infatti una tecnica del controllo sociale, le cui regole ("A") si attuano mediante la minaccia di misure coercitive ("B").

Come già riferito, non preme in questa sede entrare nel merito di queste o altre definizioni sull'essenza del fenomeno giuridico: in fondo, avremo modo di vedere come, oltre alle tradizionali forme coattive o sanzionatorie del diritto, gli odierni sistemi giuridici prevedano forme autoritative d'intervento che, nel gergo inglese, vengono chiamate *soft law*. Basti accennare per ora ai codici di auto-regolamentazione e alle opinioni o raccomandazioni delle autorità indipendenti nel campo della protezione dei dati personali.

Lasciando dunque da parte le diatribe filosofiche, occorre piuttosto precisare il livello di astrazione che connota il presente volume. Da un lato, l'attenzione va rivolta allo studio sistematico delle tecniche di cui si avvalgono gli ordinamenti giuridici, al fine di disciplinare un determinato settore, come nel caso delle tecnologie dell'informazione e comunicazione (ICT), della robotica, ecc. Da questo primo punto di vista, avendo come oggetto della propria disciplina la tecnologia, l'indagine sulle tecniche di cui si avvale il diritto, può pertanto essere convenientemente riassunta all'insegna del diritto come un saper fare "meta-tecnologico". Nonostante le assonanze aristoteliche della tesi, nella duplice apertura verso l'alto (meta-fisica), e verso il basso (meta-poietica), dello studio delle azioni umane, il livello di astrazione qui assunto, lascia impregiudicata la questione sulla natura del diritto e sui suoi fini essenziali. A partire da questo livello di astrazione, cogliamo piuttosto due diversi ordini di osservabili, con le ulteriori variabili, illustrati dalla figura 3, con cui sono chiamati a fare i conti sia i fautori del giusnaturalismo, sia del positivismo, sia i sostenitori del realismo, che dell'istituzionalismo, e via seguitando:

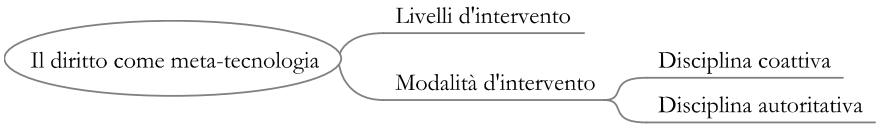


Figura 3: *Dal diritto alla tecnica*

D'altro canto, con buona pace dei formalismi giuridici, l'intento è di evidenziare come i processi tecnologici incidano e, anzi, mutino alcuni capisaldi del diritto tanto sul piano dei livelli d'intervento, ossia di ciò che tradizionalmente è espresso con la formula delle "fonti del diritto", quanto sul piano delle modalità di questo intervento. Dal punto di vista espositivo, gli osservabili e le variabili del livello di astrazione illustrato dalla figura 3 saranno introdotti di pari passo con l'esame dell'impatto della tecnologia sul diritto, per cui il passaggio dalle canoniche forme di governo all'odierna governance sarà oggetto di esame nel capitolo terzo, la trasformazione del-

le fonti del diritto nel capitolo quarto, le nuove modalità d'intervento giuridico, all'insegna del design, nel capitolo quinto, ecc.

Tuttavia, siccome molti studiosi di tecnologia ritengono che il proprio oggetto di studio non solo impatti sul diritto ma, perfino, ne vanifichi ogni modalità d'intervento, sarà opportuno proseguire l'indagine con quest'ultima tesi, riassunta all'insegna del "tecno-determinismo". Si tratta di ciò che, in sede processuale, i giuristi designano come questione pregiudiziale, ammessa la quale non è necessario addentrarsi nel merito. Vediamo in cosa consiste simile tesi.

## 1.2. *Il tecno-determinismo*

Le tesi del tecno-determinismo possono essere introdotte con il paradosso del filosofo Zenone di Elea (489-431 a.C.), a proposito di Achille e la tartaruga, ma a ruoli rovesciati. Nella versione originale, il paradosso consiste nel fatto che il pie' veloce Achille non è mai capace di raggiungere la tartaruga nella corsa alla quale egli viene sfidato: infatti, concessa alla simpatica testuggine un piede di vantaggio, quando Achille avrà raggiunto il luogo in cui si trovava precedentemente il rettile ($L_1$), quest'ultimo, per quanto poco, sarà pervenuto al punto $L_2$; e tuttavia, per raggiungere $L_2$, Achille avrà bisogno di un ulteriore lasso di tempo, durante il quale la tartaruga si sarà intanto spostata fino a $L_3$; e così via, all'infinito.

Nella versione del tecno-determinismo, invertite le parti in commedia, Achille è la tecnologia, e la tartaruga il diritto: per quanto legislatori, giudici o giuristi intendano imbrigliare l'evoluzione della tecnica, come già avvenuto ai tempi di Galileo Galilei (1564-1642), la corsa della tecnologia sarebbe troppo imperiosa e potente, per poter essere fermata da una semplice sentenza o editto. Questa opinione, estremamente popolare ancora ai nostri giorni, trova il favore di avvocati illustri e influenti: ad esempio, un distinto ricercatore di Carnegie Mellon ha dichiarato che i robot presto soppianteranno gli umani sulla terra e, anzi, la nostra specie dovrebbe cominciare a riflettere seriamente sulla possibilità di finire miseramente estinta (Moravec 1999). A sua volta, l'inventore e futurista americano Ray Kurzweil, oggi al lavoro come capo ingegnere presso Google, ha tratteggiato un imminente avvenire in *The Singularity is Near*, per cui, attraverso i progressi dell'intelligenza artificiale e la robotica, un'intelligenza di gran lunga superiore a quell'umana è destinata a emergere da qui al 2045 (Kurzweil 2008). Insomma, l'idea è che sia possibile cogliere le leggi secondo cui gli uomini sono venuti impiegando i mezzi della tecnica nel corso di centinaia di migliaia d'anni, ossia, come visto nell'introduzione di questo capitolo, dagli ominidi di *2001 Odissea nello spazio* all'odierna rivoluzione tecnologica. Come si perita di spiegare a sua volta Kevin Kelly in *Quello che vuole la tecnologia* (2011), bisogna in fondo arrendersi all'evidenza e ammettere che "maggiore il numero dei tratti isotopici che osserviamo in una data forma tecnologica, maggiore la sua inevitabilità e convivialità". E pertanto, che forza mai avranno le leggi del diritto di fronte alle leggi della tecnologia?

A ben vedere, innanzi alle tesi del tecno-determinismo e le sue varianti, non è certo il caso di negare l'innegabile, sottovalutando le caratteristiche peculiari del nostro oggetto di studio. Nel corso degli ultimi anni, è altamente significativo che gli

scienziati siano venuti discutendo dell'impatto tecnologico sull'ambiente in cui viviamo in termini di "antropocene". Secondo il neologismo coniato dal biologo Eugene Stoermer e ripreso nel 2000 dal Premio Nobel per la chimica Paul Crutzen, la formula designa l'odierna era geologica in cui l'*homo technologicus* andrebbe annoverato tra le principali concause dei nuovi equilibri climatici e strutturali del pianeta. Anche in quest'ultimo caso, però, andrebbe segnalato il ruolo che le istanze culturali, le decisioni politiche e finanche i meri pregiudizi ideologici giocano al riguardo. Basta far caso, in tema di riscaldamento globale, al peso che hanno avuto le tesi negazioniste del quarantatreesimo presidente degli Stati Uniti d'America, George W. Bush (n. 1946), nel primo decennio del XXI secolo.

A ribadire, contro ogni determinismo, la tensione dialettica esistente tra gli effetti regolativi della tecnica, il diritto e la società, basterebbe del resto riprendere la nutrita schiera di studi che, sin dal titolo dei rispettivi contributi, insiste su questa interazione: "la conformazione sociale della tecnologia" (Mackenzie e Wajcman 1985), "la costruzione sociale dei sistemi tecnologici" (Pinch e Bijker 1987), i "valori nella tecnologia" (Brey 2010), e via discorrendo.

Ma, tornando al diritto, conviene segnalare sin d'ora alcune famose decisioni giudiziarie in tema di tecnologia: ad esempio, nel caso *Sony vs. Universal City Studios* discusso, nel 1984, davanti alla Corte suprema di Washington, i giudici costituzionali erano chiamati a stabilite se la produzione e vendita dei video-registratori *Betamax* (poi soppiantati dalla tecnologia VHS) fossero legittime. Del pari, si pensi all'opinione della Corte nel caso *Grokster*, nel 2005, dove la tecnologia messa questa volta in discussione riguardava i sistemi per la condivisione dei file sulla rete di internet, noti come peer-to-peer (P2P). Ma che dire degli Aztechi, i quali, pur essendo a conoscenza della ruota, pensarono bene di non doversene servire per la costruzione delle proprie piramidi?

In sintesi, ciò che preme rimarcare con questi cenni a esperienze così distanti e disparate come le sentenze degli *justices* di Washington o la cultura *Nahuatl* dominante in Mesoamerica, è il complesso intreccio di principi e regole del diritto, istanze culturali e processi tecnologici. Lungi dal poter essere concepito come semplice rapporto unidirezionale, stante il quale la tecnologia appare la causa di effetti in senso lato sociali, bisogna prestare attenzione alle diverse forme in cui le istanze sociali possono a loro volta incidere su tempi e forme del progresso tecnologico. In fondo, se la Corte suprema americana avesse deciso altrimenti sulla legittimità costituzionale dei video-registratori o dei sistemi per la condivisione file in peer-to-peer, la storia sarebbe stata semplicemente diversa. Inoltre, anche a séguito della sentenza di costituzionalità della tecnologia P2P, è significativo il fatto che gli sviluppatori di questa tecnologia abbiano pensato bene di progettarla in modo ulteriormente decentrato (Glorioso e al. 2010; Pagallo e Ruffo 2012).

Sulla base di queste considerazioni, non bisogna naturalmente rovesciare i termini del rapporto, quasi a ricadere nella tesi eguale e contraria a quella sostenuta dal tecno-determinismo. Piuttosto, a confermare la tensione dialettica esistente tra gli effetti regolativi della tecnica e il repertorio sanzionatorio del diritto, valga un ulteriore esempio, che sarà approfondito nel prossimo paragrafo, che riguarda un po' tutti noi, avendo a che fare con la produzione e uso dell'amianto.

### 1.2.1. *Un controesempio*

In un libro apparso nel 1980, *The Social Control of Technology*, David Collingridge metteva in risalto il dilemma cui dà spesso luogo lo sviluppo della tecnica, tra la conoscenza del possibile impatto sociale di una data tecnologia e la capacità di incidere su questo medesimo impatto. "Quando il mutamento è semplice, il suo bisogno non può essere previsto; quando il bisogno di tale mutamento è ovvio, esso diventa costoso, difficile e porta via molto tempo" (*op. cit.*). Come esempio di questo dilemma, più spesso noto come "dilemma di Collingridge", basti pensare al caso dei clorofluorocarburi (CFC), vale a dire il fluido refrigerante nei cicli frigoriferi a compressione, in uso a partire dall'inizio degli anni trenta dello scorso secolo. A causa della dannosità per lo strato di ozono nella stratosfera per via dell'uso del cloro, l'impiego di questo fluido venne definitivamente bandito soltanto dopo oltre mezzo secolo, ossia con l'accordo internazionale, detto "protocollo di Montreal", siglato nel 1990.

Quattro anni più tardi, con l'accordo generale sulle tariffe e sul commercio internazionale (GATT), che avrebbe condotto alla creazione dell'organizzazione mondiale del commercio (WTO), il trattato prevedeva, all'articolo XX, alcune eccezioni alle clausole sul libero scambio, addossando però l'onere della prova sullo stato che intendesse far valere tali eccezioni a tutela della salute dei propri cittadini. Nel dicembre 1996, il governo francese approvava così un decreto con cui si vietava l'uso di (prodotti contenenti) amianto, bandendone altresì l'importazione. Di lì a un anno e mezzo, il 28 maggio 1998, il Canada iniziava le consultazioni con l'allora Comunità europea, al fine di stabilire se il bando francese dell'amianto crisotilo fosse compatibile con le clausole dell'articolo XX (b) del GATT, note come barriere tecniche al commercio (TBT). Non addivenendosi a un accordo, la disputa finiva in tribunale: il 18 settembre 2000, il Panel del WTO dava torto al governo francese, ritenendo che il suo decreto non rientrasse nell'ambito delle eccezioni TBT. Poco dopo, il 12 marzo 2001, l'organo d'appello WTO censurava però la sentenza di primo grado: non soltanto "non è stato dimostrato che la proibizione dell'amianto e di prodotti contenenti amianto siano in contrasto con gli obblighi che le Comunità europee hanno assunto con gli accordi WTO", ma l'organo d'appello cassava "l'opinione del Panel che le eccezioni TBT non si applichino al decreto francese che vieta l'uso dell'amianto e di prodotti contenenti l'amianto, stabilendo che dette eccezioni TBT legittimino il decreto francese, considerato nel suo insieme" (si v. Pagallo 2013: 150).

Senza dover semplicemente rovesciare le tesi del tecno-determinismo, ecco dunque un esempio del modo in cui il diritto come meta-tecnologia ha consentito agli europei di non essere costretti a importare o far uso di prodotti contenenti amianto.

## 1.3. *La legge di Moore (aria di famiglia)*

Può sembrare paradossale che, dopo la critica alle tesi del tecno-determinismo, il volume prosegua con un paragrafo sulla "legge di Moore", ossia, come detto nella introduzione del presente capitolo, la legge per cui, nel 1965, Gordon E. Moore, cofondatore di Intel, prevedeva che la potenza di calcolo degli elaboratori elettronici

sarebbe raddoppiata ogni anno e mezzo. Eppure, ci sono tre buoni motivi per cui il paradosso è soltanto apparente e, dunque, è possibile coniugare la critica alle tesi del tecno-determinismo con l'idea che la legge di Moore svolga un ruolo determinante nella nostra indagine.

In primo luogo, la critica alle tesi del tecno-determinismo non comporta necessariamente l'adozione della tesi eguale e contraria, stante la quale il diritto come meta-tecnologia sarebbe in grado di venire a capo di ogni problema tecnologico. Oltre i problemi del riscaldamento globale cui si è fatto cenno in precedenza, basterebbe segnalare, tra i tanti esempi possibili, l'incremento esponenziale dell'impiego dei sistemi robotici nel settore militare. Quando gli Stati Uniti invasero l'Iraq nel 2003, le forze armate americane non disponevano di alcun sistema robotico, salvo poi raggiungere all'incirca le 150 unità alla fine del 2004, diventando 2400 l'anno seguente e più o meno 12 mila al momento del ritiro delle truppe nel dicembre 2011 (v. Pagallo 2013: 55). Davanti a questa crescita esponenziale, Christof Heyns, inviato speciale delle Nazioni Uniti per le indagini nel campo delle esecuzioni extra-giudiziali, aveva richiesto nel suo rapporto del 2010 all'Assemblea Generale, che il Segretario dell'organizzazione Ban Ki-moon provvedesse a convocare un gruppo di esperti, al fine di discutere "la questione fondamentale se l'uso della forza letale possa mai divenire legittimamente del tutto automatico". Quattro anni dopo, come annunciato dalla BBC il 9 maggio 2014, si sono cominciati ad avere i primi passi in questa direzione, per cui, con le parole del servizio pubblico britannico, "i robot killer saranno oggetto di dibattito presso le Nazioni Unite" [3].

In secondo luogo, si possono criticare le tesi del tecno-determinismo e, ciò nonostante, prendere sul serio la legge di Moore, perché non si tratta di abbracciare la tesi del formalismo giuridico che nega l'impatto della tecnologia sulle categorie, sui principi o sulle regole del diritto. Anzi, si deve ammettere che siamo alle prese con (soltanto l'inizio di) una rivoluzione tecnologica, che incide alla radice sia sui livelli che sulle modalità d'intervento giuridico, senza per questo concedere l'inevitabilità di questo stesso impatto.

Infine, occorre ribadire che la legge di Moore, a differenza delle leggi della fisica o della chimica, non è una vera e propria legge ma, piuttosto, è stata (ed è tuttora) una sorta di profezia che si auto-avvera; vale a dire una sfida, o un traguardo, che vede impegnati gli esperti nel ramo dei circuiti integrati e dei micro-processori in svariati laboratori del pianeta. Indubbiamente, ci sono alcune buone ragioni, tra le quali determinate proprietà fisiche della materia, che rendono la legge possibile: nondimeno, "l'idea non spiega la sociologia di come la legge di Moore si attui o ciò che determina il tempo costante del raddoppiamento" (Brooks 2013: 238). La sequenza di incrementi nella potenza di calcolo, occorsa nelle ultime cinque decadi, non esclude in altri termini, ma integra, le ragioni politiche, economiche e culturali che favoriscono l'impiego di un dato prodotto o processo tecnologico.

La morale che si deve trarre da queste riflessioni è che possiamo accogliere la legge di Moore come un elemento cruciale dell'odierna rivoluzione tecnologica e, tuttavia, respingere le tesi estreme del tecno-determinismo. La legge chiarisce infatti

[3] Si v. *http://www.bbc.com/news/technology-27343076*.

perché tanto la già ragguardevole potenza di calcolo quanto la memoria e velocità nella elaborazione dei dati del vostro telefono siano destinate a essere solo la metà della potenza, memoria e velocità del nuovo modello che acquisterete tra diciotto mesi. La curva esponenziale di siffatta accelerazione significa, tra le altre cose, che l'onnipervasiva complessità della tecnologia è diventata, alle soglie del 2000, mille volte maggiore di quanto mai fosse agli inizi del ventesimo secolo. La serie di raddoppiamenti ha quindi reso fattibile ciò che sembrava del tutto impossibile solo pochi anni prima, dischiudendo a ritmi esponenziali nuovi orizzonti per l'ulteriore sviluppo e progresso tecnologico.

Per chiarire quest'ultimo punto, valga un ricordo di famiglia che risale a uno dei più spettacolari fiaschi nella storia di Apple, vale a dire il progetto del palmare Newton ultimato nel 1992. La squadra di esperti a Cupertino, tra cui appunto mia sorella, aveva messo a punto una sorta di proto i-Pad, dotato di riconoscimento della scrittura e, in parte, di riconoscimento vocale, con sistema per la navigazione in rete e alcuni applicativi base, come "nomi", "date" e "note", che, oltre alle mappe di navigazione, ai convertitori di valuta e al calcolatore, consentivano all'utente di produrre, gestire e condividere la propria informazione (anche) su internet. Contrariamente a quanto sarebbe accaduto nel 2010 con il lancio dell'i-Pad e, nel 2007, con l'iPhone, la realizzazione del progetto non fu coronata dal successo, anzi! Tra le ragioni del fallimento, va ricordato il prezzo del palmare e, soprattutto, il fatto che Newton fosse arrivato sul mercato con quindici anni d'anticipo. Avverso le tesi del tecno-determinismo, questo non vuol dire che il successivo impegno di mia sorella e dei suoi colleghi nella realizzazione dell'i-Pad e, tre anni prima, dell'i-Phone, fosse in qualche modo già predestinato al trionfo mondiale. Piuttosto, il ricordo di famiglia sta in realtà a segnalare come la potenza della legge di Moore contribuisca ancora una volta a gettar luce sulle complesse dinamiche del progresso tecnologico in corso.

## 1.4. *La quarta rivoluzione*

Esistono diversi modi, o livelli di astrazione, attraverso cui possiamo cominciare ad apprezzare il carattere della rivoluzione in corso, il suo ritmo esponenziale. Un primo livello è dato dalla creazione di un nuovo spazio, volta per volta indicato come cyber-spazio, internet, web o, più in generale, "infosfera" (Floridi 2009), in cui non solo possiamo sperimentare un mondo intero di nuove possibilità, ma dove vanno anche ridefiniti, o riplasmati, enti e relazioni del mondo reale, biologico o atomico. Da questo punto di vista, se gli odierni nativi digitali possono trovare difficile immaginare un mondo, quello della generazione precedente, privo di internet e cellulari – né più né meno come quella generazione, a sua volta, poteva fare fatica a immaginare il mondo dei propri genitori, privo di televisori – or bene, il passo è breve per concludere che anche la prossima generazione farà fatica a comprendere un mondo, quello odierno, nel quale viene ancora in qualche modo distinta la dimensione "online" da quella "offline", il "virtuale" dal "reale".

L'attuale rivoluzione fondata sulle tecnologie dell'informazione e comunicazione riplasma, dunque, l'ambiente in cui intessiamo le nostre relazioni. In forma ancor

più radicale, si può dire che muti la comprensione del mondo e di noi stessi, al punto che è lecito parlare di una "quarta rivoluzione" (Floridi 2014a). La prima è stata quella copernicana, alla quale ebbe modo di rifarsi ai suoi giorni anche Kant: in séguito al modello eliocentrico dell'universo messo a punto da Niccolò Copernico (1473-1543), abbiamo compreso di non essere al centro dell'universo, ma di vivere in un pianeta parte di un sistema in cui al centro c'è il sole. La seconda rivoluzione è stata quella darwiniana, a partire dall'evidenza empirica discussa in *Sull'origine della specie*: grazie alla teoria evolutiva di Charles Darwin (1809-1882), si è capito che non siamo più al centro del nostro pianeta ma, piuttosto, parte di una catena d'esseri viventi. La terza rivoluzione è stata inaugurata con gli studi sull'inconscio di Sigmund Freud (1856-1939), e trova al giorno d'oggi un più consono ambito scientifico nel campo delle neuroscienze. In sostanza, non solo non siamo più al centro dell'universo o del nostro pianeta; ma, altresì, sebbene s'inizi soltanto ora a comprendere il funzionamento del nostro cervello in rapporto alla mente (si v. ad esempio Damasio 2012), purtroppo non siamo nemmeno al centro di noi stessi!

Infine, la quarta rivoluzione è quella di cui ci occupiamo in questa sede e che, tra i tanti precursori, può essere convenientemente fatta risalire al grande matematico inglese Alan Turing (1912-1954). Ciò che l'odierna rivoluzione ha messo in chiaro è la nostra natura di organismi informazionali interconnessi, che condividono sia con gli organismi biologici, sia con gli enti e agenti artificiali, un ambiente globale fatto d'informazione. Si tratta, come detto poc'anzi, di ciò che Floridi invita a pensare in termini di "infosfera". Per esprimere il concetto con il filosofo e matematico americano, nonché padre della cibernetica, Norbert Wiener (1894-1964), bisogna prestare attenzione al fatto che "l'informazione è informazione, non è né materia né energia. Nessun materialismo che non ammetta questo può sopravvivere ai giorni nostri" (Wiener 1950: 155).

Possiamo lasciare tra parentesi in questa sede i più generali profili teoretici e pratici della quarta rivoluzione, secondo il modello illustrato sopra con la figura 1 del § 1.1. Piuttosto, stante l'oggetto della nostra indagine, converrà concentrarci sui riflessi giuridici della rivoluzione in corso, distinguendone quattro aspetti che riguardano i processi cognitivi del diritto, i suoi istituti, le tecniche e le istituzioni. La figura 3 del § 1.1.3 dovrà pertanto essere integrata con una nuova figura che illustri i nuovi osservabili dell'analisi, quelli della figura 4 presentata qui sotto.

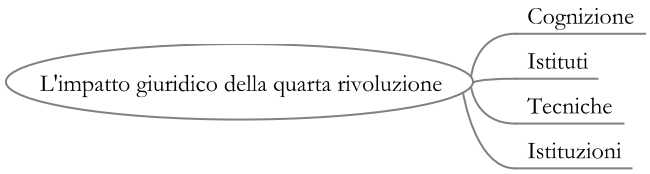


Figura 4: *Dalla tecnologia al diritto*

A continuazione, le quattro sezioni che concludono il presente capitolo saranno rispettivamente dedicate a ciascuno degli osservabili della figura 4, ossia i processi cognitivi del diritto (§ 1.4.1), i suoi istituti (§ 1.4.2), le tecniche (§ 1.4.3), e le istitu-

zioni del diritto nell'era delle società ICT-dipendenti (§ 1.4.4). Su queste basi, saremo in grado di raffinare ulteriormente la nostra analisi per concentrarci, nel capitolo secondo, sul tema della complessità del diritto.

### 1.4.1. *Cognizione*

Il settore che tradizionalmente si occupa dell'impatto tecnologico sui "fondamenti cognitivi del diritto" (Caterina 2008), è l'informatica giuridica (Durante e Pagallo 2012). Qui, particolare rilevanza assume, da un lato, l'informatica giuridica "documentaria" che riguarda il trattamento automatizzato delle fonti di cognizione dell'ordinamento e il reperimento dei testi delle leggi e delle sentenze. D'altro canto, l'informatica giuridica "decisionale" si occupa delle fonti di produzione dell'ordinamento tramite l'elaborazione informatica dei processi logico-formali presenti nel procedimento legislativo e nelle decisioni giudiziarie. Più in particolare, quest'ultimo ambito studia tanto la tecnica della produzione di norme giuridiche, sostituendo ad esempio il linguaggio naturale del legislatore con il linguaggio formale della logica proposizionale di Boole, quanto la tecnica dell'interpretazione delle disposizioni di diritto positivo, mediante l'elaborazione e uso di banche dati con le quali processare l'informazione contenuta nella legislazione, nella giurisprudenza o la dottrina.

Al riguardo di quest'ultimo sotto-settore, detto anche "giuri-tecnica", un'attenzione speciale va poi riservata al ruolo svolto dalle ricerche nel campo dell'intelligenza artificiale e, al suo interno, delle cosiddette ontologie giuridiche. Si tratta dell'ambito in cui è dato maggiormente apprezzare l'impatto della tecnologia sui processi cognitivi del diritto, in quanto l'obiettivo di queste ricerche è che perfino una macchina sia in grado di capire e processare l'informazione giuridica! Per quanto l'intento possa apparire fantascientifico a qualche lettore (o studente) inesperto, questo è il (mio) pane quotidiano di progetti e studi relativi ai temi della sicurezza in rete, alla tutela dei dati personali, o alla protezione dei diritti di proprietà intellettuale, per cui è forse il caso di spendere sin d'ora qualche parola in materia.

Al fine di coadiuvare umani e agenti artificiali nel loro lavorio giuridico, occorre modellizzare nozioni tradizionalmente impiegate nel campo, come ciò che è "dovuto", "proibito", o "permesso", tramite la formalizzazione delle norme, diritti e doveri, nei diversi settori del diritto civile, penale, amministrativo, ecc. Tale formalizzazione richiede di distinguere dai requisiti ontologici, vale a dire la parte dell'ontologia che, tramite l'uso di tassonomie, contiene tutti i concetti rilevanti del settore, i vincoli ontologici o insieme delle regole e limiti con cui quegli stessi concetti vanno rappresentati. Un sistema esperto deve di qui processare l'informazione giuridica e risolvere i problemi di applicazione della normativa vigente, mediante la concettualizzazione di classi, relazioni, proprietà e istanze che appartengono a quello specifico settore. Tanto più quest'ultimo si presta a un approccio dall'"alto verso il basso", ossia, tramite l'applicazione dei concetti normativi di base, quali "validità", "obbligazione", "proibizione", ecc., tanto più l'automazione del ragionamento giuridico sarà possibile con la quantificazione dei dati.

Tuttavia, come usa dirsi, il diavolo è nei dettagli: l'interpretazione dei concetti dipende infatti, molto spesso, dal contesto in cui tali concetti devono essere applica-

ti. Un esempio è dato dal settore della protezione dati personali, proprio perché quest'ultima nozione, al pari di altre – come "misure di sicurezza" o "controllore dei dati" – non possono essere del tutto de-contestualizzate. Anzi, basterebbe pensare con gli esperti del ramo, alle sfide poste dai temi della sicurezza, per cui "l'unico sistema [informatico] realmente sicuro è quello che sia stato spento, messo dentro a un blocco di cemento e sigillato a piombo in una stanza attorniata da guardie giurate – e anche così avrei i miei dubbi" (in Garfinkel e Spafford 1997: 9).

Or bene, per affrontare queste e simili difficoltà dell'automazione, soccorrono per fortuna alcuni accorgimenti metodologici. È sufficiente menzionare, in questo paragrafo, il "ciclo generatore di test" proposto ai suoi giorni dallo scienziato americano e Nobel dell'economia, Herbert Simon (1916-2001). Nel suo pionieristico contributo su *Le Scienze dell'artificiale* (1969), Simon raccomandava di adottare un approccio "dal basso verso l'alto", vale a dire scomponendo i progetti in blocchi funzionali, in modo da generare attraverso il test modi alternativi per venire a capo dei problemi e testarli, appunto, sulla base dell'insieme dei requisiti e vincoli ontologici. Con le parole di Simon, "importanti conseguenze indirette verranno alla luce e soppesate. Le decomposizioni alternative del progetto corrispondono a diversi modi di suddividere le responsabilità per il design finale, tra generatori e test" (*op. cit.*, ed. 1996: 128).

Tra l'inerzia degli scettici e l'astratto ottimismo dei tecno-deterministi, il risultato è che sia possibile individuare ancora una volta una via di mezzo. Affrontando la ricerca attraverso le sue componenti funzionali, è possibile specificarne la serie di problemi elementari da affidare ai sotto-gruppi del progetto. In ragione della soluzione che viene, volta per volta, trovata per ciascuno dei problemi parziali, è dato infatti processare un numero incrementale d'informazione giuridica con cui procedere allo sviluppo ulteriore di sistemi esperti e applicazioni dell'intelligenza artificiale al mondo del diritto. Si tratta in fondo di uno dei fili conduttori del presente volume, con il quale saremo chiamati a misurarci nei capitoli conclusivi del libro.

### 1.4.2. *Istituti*

Il secondo insieme di osservabili della figura 4 concerne due classi di variabili. Da un lato, il riferimento va alle nuove fattispecie dell'ordinamento che i legislatori, sia sul piano nazionale sia internazionale, hanno introdotto per via della rivoluzione tecnologica. Si pensi innanzitutto al settore penale dove, stante il principio di legalità e il divieto di analogia[4], i legislatori hanno dovuto introdurre tutta una nuova serie di reati, e cioè i "reati informatici", sin dall'inizio degli anni novanta: il 1993, per l'esattezza, nel caso dell'Italia. Qui, tuttavia, bisognerebbe ulteriormente distinguere tra i nuovi crimini informatici in senso stretto e, come si esprime il legislatore italiano al secondo comma dell'articolo 253 del codice di procedura penale, il fatto che "le cose sulle quali o mediante le quali il reato è stato commesso" abbiano natura

[4] Per quanto riguarda il principio di legalità, si pensi al disposto dell'articolo 25 della Costituzione italiana, nonché all'articolo 7 della Convenzione europea sui diritti dell'uomo del 1950. Per ciò che riguarda invece il divieto di analogia in sede penale, il rimando va all'articolo 14 delle disposizioni preliminari al codice civile italiano, ossia le cosiddette "preleggi".

informatica. Come annota perspicacemente uno dei maggiori esperti del settore, l'avvocato torinese Carlo Blengino, è lecito dubitare che si possa definire come crimine informatico "il truffatore del XXI secolo [che] venderà la fontana di Trevi utilizzando un accattivante sito internet" o "se nel corso di una rissa sfascio lo smartphone del mio avversario, danneggiando inevitabilmente le informazioni, i dati e i programmi in essi contenuti" (Blengino 2012: 220). Piuttosto, l'attenzione va posta sui reati necessariamente informatici, quelli, cioè, che sarebbero impensabili senza l'impiego della tecnologia in questione, come ad esempio nel caso del danneggiamento e la frode informatica, l'accesso abusivo e le violazioni della corrispondenza elettronica, il falso informatico di cui all'articolo 491 *bis* del codice penale, e via discorrendo.

D'altro canto, la rivoluzione tecnologica ha contribuito a riplasmare vecchi istituti: qui l'esempio forse più calzante è offerto, oltre al diritto alla privacy e con la tutela dei dati personali, dal vecchio diritto d'autore. Introdotto per la prima volta nel Regno Unito con lo Statuto d'Anna del 1709, il punto di riferimento normativo su scala internazionale è stato rappresentato, per più di un secolo, dalla Convenzione di Berna del 1886 (mentre, in Italia, il richiamo va tuttora alla legge 633 del 22 aprile 1941, sia pure raffazzonata, in modo tormentato, nel corso degli ultimi anni). Tutto ad un tratto, la vecchia normativa è infatti rimasta spiazzata dalla diffusione di una tecnologia, quella digitale, che tra le tante cose cancella la stessa distinzione ontologica tra originale e copia, rendendo il vecchio diritto d'autore, o copyright, una questione di accesso, disponibilità e controllo sul flusso di informazioni in 0 e 1. Poco dopo la prima ondata di legge penali in materia di crimini informatici, si è assistito di qui, a partire dalla metà degli anni novanta, al convulso susseguirsi di una serie d'interventi normativi: del 1996 sono gli accordi internazionali dell'organizzazione mondiale della proprietà intellettuale (WIPO), il cui fine era di impedire "che i membri del pubblico possano accedere alle opere [protette dal copyright per le registrazioni sonore e i fonogrammi] da un luogo e tempo scelto individualmente da costoro", come recitano sia l'articolo 8 del trattato WIPO sul copyright sia l'articolo 14 del trattato WIPO sugli spettacoli e i fonogrammi.

Sul piano nazionale, nel 1998, il Congresso nordamericano emendava a sua volta il *Digital Performance Rights in Sound Recordings Act* varato solo tre anni prima, con il *Digital Millennium Copyright Act* (DMCA) e il *Sonny Bono Act* sull'estensione dei diritti di esclusiva. È oltremodo indicativo che dall'originario termine di quattordici anni stabilito dallo Statuto d'Anna e il *Copyright Act* americano del 1790, si sia passati a ventotto anni nel 1831, a ulteriori ventotto anni di rinnovo nel 1909, a cinquant'anni d'esclusiva dopo la morte dell'autore nel 1976, fino agli odierni settant'anni introdotti con il *Sonny Bono Act* del '98. A sua volta, in Europa, il legislatore approntava la prima direttiva comunitaria su "copyright e diritti connessi nella società dell'informazione" nel 2001, di lì a poco emendata, nel 2004, con la direttiva 48 sul "rispetto dei diritti di proprietà intellettuale", cui avrebbe fatto séguito un ulteriore tentativo di riforma, poi fallito, nel 2007. Nel frattempo, il legislatore di Washington non è stato certo a guardare: tra le innumerevoli modifiche e novità, mi limito a segnalare il *Technology, Education, and Copyright Harmonization Act* (2002), il *Family Entertainment and Copyright Act* (2005), il *Prioritizing Resources and Organization for Intellectual Property Act* (2008), il *Copyright Cleanup, Clarification, and Corrections Act* (2010), ecc.

Insomma, a vent'anni dalle prime modifiche della vecchia Convenzione di Berna, si può dire che i legislatori non abbiano tuttora trovato il proverbiale bandolo della matassa se, ancora, nel 2013 c'è stato un ennesimo tentativo (fallito) di modificare il quadro internazionale attraverso un nuovo trattato, detto ACTA, e se all'inizio del 2014 venivano avviate le consultazioni a livello europeo per una nuova direttiva in materia. Lasciando per ora in disparte le ragioni del perché i legislatori, nazionali e internazionali, non abbiano trovato un modo soddisfacente per disciplinare il fenomeno, rimane però chiara la morale del presente paragrafo, e cioè come la tecnologia provochi problemi giuridici inediti, trasformando vecchie fattispecie o proponendone delle nuove [5].

### 1.4.3. *Tecniche*

Le tecniche cui si fa riferimento in questo paragrafo, come terzo osservabile della figura 4, non vanno tanto riferite alla tecnica di produzione delle norme giuridiche, o alla tecnica con cui tali disposizioni vanno interpretate, secondo quanto emerso sopra, nel § 1.4.1, a proposito degli studi d'informatica giuridica. Il richiamo va piuttosto a quanto detto nel § 1.1.3, a proposito della tesi kelseniana del diritto come tecnica e, più specificatamente, come tecnica del controllo sociale che si attua mediante la minaccia di misure coercitive: "se A, allora B". Infatti, uno degli aspetti più rilevanti della rivoluzione tecnologica e del suo impatto sugli ordinamenti giuridici concerne la crescente inefficacia dell'approccio, ad esempio, nell'ambiente della rete, su internet.

Tra i tanti casi, basti riferire quello dello "spamming", la posta indesiderata che ciascuno di noi trova quotidianamente nella propria casella di posta elettronica. Ancora una volta i legislatori sono intervenuti al riguardo, minacciando anche pene severissime: si pensi all'articolo 13 della direttiva europea 58 del 2002, in materia di comunicazioni elettroniche e privacy; ma, soprattutto, il *CAN-SPAM Act* statunitense del 2003. Infatti, malgrado la severità delle pene e il fatto che, di tanto in tanto, qualche malfattore venga arrestato – come occorso, nell'agosto 2011, quando Sanford Wallace, noto anche come "Spamford Wallace", venne sottoposto ad arresto a Las Vegas da parte degli agenti dell'FBI – non si può dire certo che il problema sia stato risolto.

Più in generale, ci sono tre ragioni principali per le quali il tradizionale apparato sanzionatorio del diritto appare spesso inefficace nella rete: innanzitutto, e nonostante l'accennato arresto di Spamford Wallace, risulta talora difficile, se non impossibile, identificare il responsabile dell'atto sanzionato dalla legge. Ciò non vale soltanto per casi di spamming, furti d'identità digitali, o violazioni del copyright, ma anche, per non dire soprattutto, per i nuovi scenari della cyber-guerra. Basti pensare agli attacchi DoS subiti dall'Estonia tra l'aprile e il maggio 2007, che paralizzarono

[5] Ad onor del vero, non si tratta di un problema che attiene soltanto alla disciplina dei processi tecnologici, come le acrobazie ermeneutiche dell'Autorità indipendente italiana per le garanzie nelle comunicazioni (AGCOM) hanno illustrato abbondantemente in questi ultimi anni, proprio in materia di copyright. Infatti, basterebbe aggiungere come nel corso di quarantacinque anni (1968-2014), il legislatore italiano non abbia ancora capito come governare l'università di massa.

la piccola repubblica baltica e che attendono, tuttora, di stabilire chi debba essere considerato responsabile di tali attacchi.

In secondo luogo, internet travalica di solito i tradizionali confini giuridici degli stati, per cui non è sempre chiaro o, anzi, può essere estremamente difficile stabilire all'atto pratico, quale sia la legge da dover rispettare. Le leggi non soltanto possono essere confliggenti per ciò che riguarda, poniamo, la libertà d'espressione, la protezione dei dati personali, la diffamazione o la pornografia; ma, capita spesso che gli utenti preferiscano seguire le consuetudini e usi della rete, piuttosto che le regole di un legislatore lontano. Si tratta di un fenomeno ampiamente studiato (Murray 2007: 126-164; Schultz 2007: 151; Reed 2012: 82; ecc.). La possibilità di scelta tra ordinamenti diversi che, prima dell'era di internet, era appannaggio esclusivo delle imprese multinazionali, è stata per così dire democratizzata, estendendosi a raggiera tra gli utenti.

In terzo luogo, infine, devono rimarcarsi i risvolti psicologici nell'uso della rete, per cui il comando del legislatore risulta disatteso vuoi perché il medium sembra garantirne l'impunità, vuoi perché in rete non appaiono illeciti comportamenti che invece possono sembrare tali nel mondo reale, vuoi perché il navigante d'internet, semplicemente, ritiene errata la regola stabilita dal legislatore in mala fede o ignorante.

Naturalmente, tanto i legislatori nazionali e internazionali, quanto le imprese a tutela dei propri (presunti) diritti, sono corsi ai ripari fin dalla metà degli anni novanta del secolo scorso. Alla tecnica del diritto come mezzo di controllo sociale che fa leva sulla minaccia di misure coercitive si è affiancata – o la si è sostituita con – la tecnica di immettere le regole del diritto nella tecnologia stessa. Siccome l'argomento sarà oggetto specifico di un capitolo del libro, il quinto in materia di design, basti qui chiarire il punto con due esempi. Il primo riguarda l'autotutela nel settore privato ed è noto a qualunque tra i lettori con qualche dimestichezza della galassia Apple: si tratta dell'uso di tecniche protettive DRM per tutti i contenuti (video, musicali, ecc.) sottoposti a tutela del copyright. Per quanto riguarda invece il settore pubblico, il secondo esempio è dato dal principio della "privacy tramite design", per cui, ai sensi del considerando 46 della direttiva europea 46 del 1995 in materia di tutela dei dati personali, si "richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento".

### 1.4.4. *Le società ICT-dipendenti*

L'ultimo osservabile della figura 4 riguarda i mutamenti istituzionali che sono stati favoriti, o in senso lato prodotti, dalla rivoluzione tecnologica in corso. Come segnalato fin dall'introduzione del libro, sulla scorta delle indicazioni di Floridi (2014a), siamo alle prese con una vera e propria rivoluzione, perché è radicalmente mutato il rapporto che le società umane hanno con le tecnologie dell'informazione e comunicazione (ICT). L'inizio della storia può infatti essere fatto risalire al momento in cui gli uomini hanno cominciato a fare uso della più basica delle ICT, la scrittura. Questa è stata appunto la condizione che ha reso possibile il ricordo dei tempi passati, e cioè la storia stessa. Sul fronte occidentale, si è già detto che questo snodo

cruciale tra oralità e scrittura è ben raffigurato dall'ambivalenza di Platone: sebbene il filosofo abbia pensato bene di mettere per iscritto le sue opere – i dialoghi – egli nondimeno afferma, nella famosa *Lettera VII* (341c5-d2), che su taluni punti chiave della sua dottrina "non c'è un mio scritto, né ci sarà mai". Questa ambivalenza trova la sua forma plastica nel mito di Theuth, descritto da Platone nel *Fedro*, in cui la divinità dona a Thamus, sovrano d'Egitto, l'arte della scrittura[6]. Il rimando va a una tecnica che, sul fronte orientale, ha prodotto il "più antico libro del mondo", il *Libro dei Mutamenti*, o *I Ching* – retrodatabile al primo o, forse anche, secondo millennio prima di Cristo – che, ancora oggi, rappresenta un punto di riferimento essenziale della cultura e saggezza cinese.

Nel corso dei secoli, tanto la civiltà occidentale quanto quella orientale, benché abbiano certamente fatto uso di ICT, sono tuttavia dipese da altri tipi di tecnologia; soprattutto, quelle relative alle fonti di energia o concernenti altre risorse vitali, come quelle idriche, minerarie, agro-alimentari, ecc. Ciò non significa, evidentemente, che il settore delle ICT sia rimasto inerte: basterebbe ricordare l'invenzione della stampa a caratteri mobili di Johann Gutenberg (ca. 1394-1468). Eppure, è soltanto nei decenni a noi più vicini che, prima in occidente (Stati Uniti), poi in oriente (Giappone, Sud Corea), le società sono venute progressivamente dipendendo dall'uso delle ICT. Per cogliere il trend, basta qualche cifra approntata dalla Banca mondiale e dalla Conferenza delle Nazioni Unite sul commercio e lo sviluppo, per cui più del 20% dell'aumento del prodotto interno lordo (PIL), che si è avuto nel pianeta negli ultimi anni, è dipeso da internet, mentre oltre il 50% dei servizi per l'esportazione dipendono oggi dall'impiego d'ICT (Lee-Makiyama 2014: 88). In uno studio messo a punto dalla Commissione europea[7], si è inoltre calcolato che il settore delle ICT è passato, negli Stati Uniti d'America, dall'8% del PIL nel 2007, a oltre il 9% nel 2010, raggiungendo in questo modo, oramai, le già ragguardevoli cifre del settore petrolifero. In Europa, i dati sono sensibilmente più bassi (poco più del 5% nel 2007, il 6% nel 2010), a causa della diversa distribuzione degli investimenti nella ricerca e sviluppo che hanno visto, nel 2009, la Germania primeggiare con il 21,24% del totale complessivo dell'Unione, la Francia con il 17,99%, il Regno Unito con l'11,76%, la Finlandia con l'11,43%, e solo quinta l'Italia all'8,53%. Senza addentrarci ulteriormente nelle statistiche del rapporto, le conclusioni sono significative: "il potenziale di crescita del mercato interno dei paesi industrializzati come gli Stati Uniti, l'UE o il Giappone, stante diversi fattori come le tendenze demografiche, dipenderà quasi esclusivamente dal progresso tecnologico (guadagni di produttività)" [8].

---

[6] Vale la pena ricordare la risposta di Thamus a Theuth: " O ingegnosissimo Theuth, c'è chi è capace di creare le arti e chi è invece capace di giudicare quale danno o quale vantaggio ne ricaveranno coloro che le adopereranno. Ora tu, essendo padre della scrittura, per affetto hai detto proprio il contrario di quello che essa vale. Infatti, la scoperta della scrittura avrà per effetto di produrre la dimenticanza nelle anime di coloro che la impareranno, perché fidandosi della scrittura si abitueranno a ricordare dal di fuori mediante segni estranei, e non dal di dentro e da se medesimi" (*Fedro*, tr. it. a cura di Giovanni Reale, 274c-275b).

[7] Cfr. *http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/KKAH12001ENN-chap4-PDFWEB-4_0.pdf*.

[8] Si v. a p. 81 del documento citato nella nota precedente.

Per approfondire il significato di questa dipendenza, tornano utili due dei temi introdotti precedentemente, a proposito della distinzione platonica tra società primitive e società opulente (§ 1.1), e la creazione di un nuovo mondo oltre quello tradizionale, definibile con il neologismo di Floridi come infosfera (§ 1.4). Per quanto attiene al primo punto, è certamente vero che la natura ICT-dipendente delle attuali società comprende i beni voluttuosi della società opulenta: il lettore pensi alle applicazioni del suo telefono, alla propria pagina Facebook, ecc. Ma, la dipendenza di cui si tratta ha anche, se non soprattutto, a che fare con le esigenze primarie del funzionamento di queste società, nel senso che, ai fini dell'adattamento e sopravvivenza della specie, bisognerà aggiungere alle classi socratiche degli agricoltori, muratori, tessitori e calzolai, la figura dell'informatico!

Infatti, passando alla seconda considerazione circa la natura ICT-dipendente delle odierne società, converrà riflettere sul dato che molte delle attività essenziali relative al loro funzionamento, sono progressivamente emigrate nell'infosfera. Ciò vale per l'acqua potabile, l'elettricità, il sistema dei trasporti, le banche o il servizio fognature. Lo scenario apocalittico proposto dal film *Die Hard 4* con Bruce Willis nel 2007 è tutt'altro che un film di fantascienza se, un paio d'anni or sono, l'allora segretario alla difesa nordamericano, Leon Panetta, metteva in guardia sul fatto che un attacco informatico sarebbe in grado di mettere in ginocchio uno stato intero, potendo far "deragliare treni passeggeri, contaminare i pozzi d'acqua delle maggiori città, o spegnere le centrali elettriche di molte parti del paese" (in Schmidt e Cohen 2013: 104).

Sono due gli aspetti giuridici di questo mutamento epocale che preme evidenziare in questa sede: da un lato, con la crescente ICT-dipendenza delle odierne società aumenta di pari passo la natura globale e interconnessa dei problemi da affrontare. Oltre alle questioni del riscaldamento globale, la deforestazione in Amazzonia o la disciplina dei mercati e dei flussi finanziari del pianeta, è il caso delle decisioni da dover assumere sul futuro d'internet, sia per le questioni di infrastruttura e accesso alla rete, che per i problemi d'ordine logico, relativi al dominio nomi, protocolli e altri standard del sistema, per giungere ai contenuti e all'impatto sociale della rete medesima. D'altra parte, tanto più i problemi da dover fronteggiare nell'ambito delle società ICT-dipendenti hanno natura globale, tanto meno i tradizionali confini giuridici e politici degli stati sovrani potranno fornire la scala o dimensione adeguata per affrontare questi stessi problemi. Per via della loro crescente complessità, il risultato è che molti dei consueti modi di concepire le modalità di governo, la rappresentanza politica, la partecipazione civica, o la responsabilità giuridica, non sono all'altezza del compito.

Nel prossimo capitolo, avremo modo di occuparci del concetto che, più di altri, riassume le sfide giuridiche delle odierne società ICT-dipendenti, e cioè la nozione di "complessità". Soltanto una volta svolto questo tema attorno ai due osservabili della figura 3, sarà possibile fare ritorno al compito del diritto di disciplinare i processi tecnologici in corso. Nel capitolo terzo, l'attenzione andrà infatti alle modalità d'intervento, secondo il passaggio che conduce dalla nozione di governo a quella nuova (e significativamente intraducibile in italiano) di governance; mentre, nel capitolo quarto, si tratterà di concentrarci sui livelli di intervento, le cosiddette fonti del diritto.

# II.
# *Complessità*

"La complessità non è altro che la scienza della sorpresa"
John CASTI

Abbiamo concluso il capitolo precedente, osservando come i problemi giuridici posti dall'odierna rivoluzione tecnologica possano essere riassunti con una parola sola, "complessità". Il guaio è, però, che la nozione risulta a sua volta complessa: per illustrare il punto, mi rifaccio a quanto occorso tempo fa a Seth Lloyd, attualmente professore di ingegneria meccanica al M.I.T. di Boston. Prima ancora di diventare uno dei più noti protagonisti dell'odierno dibattito su computer quantistici, scienza fisica e filosofia digitale, Lloyd era stato invitato nel 1999 al prestigioso Istituto per lo studio dei sistemi complessi a Santa Fe, New Mexico, per una conferenza dal significativo titolo *Trentuno misure diverse della complessità* (si v. Lloyd 2006: 171). Tale fu l'accoglienza riservata alla relazione che, poco dopo, non solo lo studioso si vide costretto a metter per iscritto il saggio, poi pubblicato nel 2001 sulla "IEEE Control System Magazine", ma nel frattempo le misure di complessità erano salite da trentuno a quarantadue!

Come sanno gli studiosi della materia, oltre la complessità, esistono nondimeno le riduzioni della medesima: nel caso di Lloyd, le diverse forme di misurare la complessità avrebbero dovuto essere suddivise in quattro categorie. L'intento può essere a volte quello di misurare la difficoltà che s'incontra nel descrivere un dato fenomeno; oppure, può concernere la difficoltà di eseguire il programma con il quale lo si intende riprodurre; nel qual caso, si tratta di valutare ulteriormente il grado di organizzazione del sistema, o la sua auto-organizzazione o capacità d'adattamento. Approfondendo soprattutto i primi tre versanti della ricerca, Lloyd si soffermava, così, sulla nozione di "profondità logica" proposta da Charles Bennett negli anni Ottanta, ma in realtà approfondita vent'anni prima sia da Ray Solomonoff sia da Gregory Chaitin, su cui avremo modo di tornare più sotto (§ 2.1). In sostanza: l'intenzione era quella di misurare la complessità dell'oggetto di studio in ragione del programma informatico che, nel minor numero di bit, riproduca al computer l'oggetto in questione.

Dopo questa (prima) definizione di complessità, Lloyd sottolineava poi come il suo maestro, Heinz Pagels, avesse avuto di mira una teoria ancor più specifica, in grado di dar conto della complessità dei sistemi fisici in termini di energia. Segnala-

te le difficoltà cui va incontro la teoria algoritmica di Solomonoff e Chaitin, nel rappresentare oggetti ad alta complessità informativa e che, però, sono difficili da riprodurre casualmente, maestro e allievo sviluppavano un concetto di complessità come "profondità termodinamica", al fine di stabilire la distanza che separa un sistema dal suo stato di massima entropia. In collaborazione con uno dei padri fondatori del Santa Fe Institute, Murray Gell-Mann, Lloyd è venuto di qui affinando queste idee con il concetto di "complessità effettiva", dove lo scopo è, in questo caso, di misurare la quantità dell'informazione necessaria per descrivere le regolarità di un sistema determinato. Sul piano epistemologico, la conclusione alla quale è giunto il fisico statunitense non è troppo distante dall'approccio metodologico sui livelli di astrazione, illustrato qui sopra al § 1.1.2. Con le parole di Lloyd, la misura della complessità adottata deve necessariamente mutare "a seconda di ciò che vogliamo evidenziare tra le caratteristiche di un sistema complesso" (Lloyd 2006: 175). Cosa vogliamo, dunque, evidenziare nel caso di quel sistema complesso che è certamente il diritto?

Al riguardo, tornano utili le riflessioni svolte nel § 1.1.3 e illustrate con la figura 3 sul diritto come meta-tecnologia. In ragione della complessità del fenomeno giuridico, è dato infatti approfondire le considerazioni relative alla natura del diritto, in rapporto alle modalità e livelli d'intervento normativo, insistendo su tre diversi piani d'indagine: la complessità del diritto come informazione, come fenomeno d'emergenza dalla complessità, e come complessità del sistema. A differenza dell'ordine espositivo adottato nel capitolo precedente, il lettore ben può chiedersi perché, assunto il livello di astrazione che concepisce il diritto in termini di complessità, questo capitolo affronti prima le modalità e, poi, i livelli d'intervento normativo. In realtà, si tratta di una mera sequenza a fini didattici, imposta dalla natura diacronica di ogni esposizione, per cui vale l'assunto che l'ordine dei fattori, neanche in questo caso, incida sul prodotto. Sul piano sincronico, i nuovi osservabili dell'indagine sono illustrati dalla prima figura del presente capitolo:

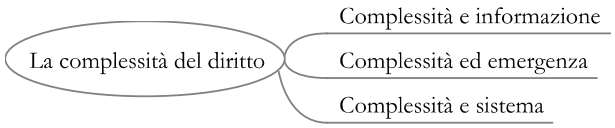


Figura 5: *Il diritto come meta-tecnologia nella società complessa*

Alla luce dei tre livelli di complessità riassunti dalla figura 5, l'indagine di questo capitolo è suddivisa pertanto in altrettanti paragrafi. Innanzitutto (§ 2.1), l'attenzione andrà rivolta alla teoria algoritmica della complessità proposta dal già citato matematico americano Gregory Chaitin (n. 1947); teoria che servirà a gettare luce su quella tradizione filosofica che, a vario titolo, ha inteso rappresentare il diritto in termini di informazione. Questo livello d'analisi consentirà inoltre di capire la disparità di vedute attorno al fenomeno giuridico che, ancora oggi, anima il dibattito. Dopo di che, nel § 2.2, l'indagine si soffermerà sulla teoria della complessità messa a punto dal filosofo austriaco e Nobel dell'economia, Friedrich Hayek (1899-1992).

Riprendendo la sua distinzione tra "taxis" e "kosmos", progettualità politica e ordini spontanei – ossia, ciò che i giuristi spesso designano come fonti atto e fonti fatto – il proposito è di esporre un primo punto di vista normativo su come affrontare in termini giuridici i nodi della complessità. Infine, nel § 2.3, l'analisi verterà sui profili sistemici della complessità giuridica, secondo uno dei temi più popolari, tra gli anni sessanta e ottanta del secolo scorso, tra i cultori della teoria dei sistemi e soprattutto con l'opera del sociologo tedesco Niklas Luhmann (1927-1998). Su queste basi, ritorneremo su uno dei problemi chiave rilevati a conclusione del capitolo precedente, e cioè come la rivoluzione tecnologica sollevi questioni che, più spesso, investono l'ordinamento nel suo complesso. Le ragioni che hanno in questo modo suggerito di spostare il livello d'intervento giuridico dal piano tradizionale del governo a quello globale della odierna governance, saranno approfondite nel capitolo terzo.

## 2.1. *Le vie dell'informazione*

Il primo osservabile dell'analisi su complessità, diritto e informazione, richiede una premessa su quest'ultimo concetto poiché, al pari di "complessità" e "diritto", anche il termine "informazione" risulta a sua volta complesso. Per giustificare l'affermazione, basti dire che, quando alla fine degli anni quaranta del secolo scorso furono poste le basi dell'odierna teoria scientifica (o matematica) dell'informazione, il padre fondatore, Claude Shannon (1916-2001), e il già ricordato padre della cibernetica, Norbert Wiener, ne davano due letture differenti. Per Wiener, l'informazione avrebbe dovuto intendersi come ciò che si oppone all'entropia, dato che l'attenzione si dirige alla quantità d'informazione guadagnata attraverso un messaggio determinato. Per Shannon, invece, l'informazione appariva direttamente proporzionale all'entropia dato che, quanto più un messaggio risulta casuale, o inaspettato, tanto maggiore la quantità dell'informazione trasmessa (Shannon e Wiener 1949, ed. it. 1971).

In questa sede, il livello di astrazione che s'intende assumere è quello che si spera più propizio per comprendere il significato dell'informazione come informazione giuridica; primo passo per cogliere il senso in cui questa stessa informazione debba poi intendersi come più o meno complessa.

Da questo punto di vista, conviene pertanto soffermarsi su quel particolare tipo d'informazione detto informazione semantica, vale a dire l'informazione basata su dati dotati di significato (Floridi 2012: 24). I dati possono essere a loro volta intesi come mancanza di uniformità nel mondo reale, a cui attribuiamo appunto un significato determinato. Ciò vale anche per le difformità dei segnali fisici, come accadeva con il punto e la linea nel vecchio alfabeto Morse; ma anche tra simboli, come accade invece con le lettere dell'alfabeto. Per amore di sintesi, questi diversi livelli di disparità sul piano dei dati sono qui resi con l'unico termine di "realtà", rispetto alla quale possono distinguersi tre tipi diversi d'informazione (Floridi 2005: 293).

In primo luogo, abbiamo l'"informazione come realtà" – ICR o Info1. Questo tipo di informazione non ha necessariamente valenza semantica, nel senso che può riferirsi ai dati del mondo reale dotati di significato, indipendentemente dal fatto che, sulla base di essi, un essere intelligente trasmetta o produca informazioni. Con l'esempio di Floridi (2012: 39), è il caso dei "cerchi concentrici visibili nel

legno della sezione di un tronco d'albero". Nondimeno, oltre all'informazione ecologica o ambientale, possiamo pensare ad altri tipi di ICR, o Info1: un esempio è dato proprio dalla tradizione della filosofia del diritto e, in special modo, dalle scuole del diritto naturale che, fin dai tempi di Platone e Aristotele, hanno inteso ricavare dalla natura delle cose i principi del diritto. Più di recente, forme di ICR sono state messe in risalto nell'ambito degli studi di neuro-diritto e con la psicologia evolutiva, per cui concetti basici del diritto e dell'etica sarebbero per così dire "cablati" nei nostri cervelli, per ciò stesso aprendo la strada all'evoluzione culturale (si v. Pinker 2007).

In secondo luogo, il riferimento va all'"informazione per la realtà" – IPR o Info2. Qui, abbiamo a che fare con l'informazione intesa come insieme di regole o istruzioni, che determinano il modo di essere di altre entità. Un esempio è offerto dal DNA o informazione genetica: nel campo giuridico, bisogna invece prestare attenzione alle varie accezioni del diritto in chiave giuspositivistica, le quali trovano nel padre della scienza giuridica e politica moderna, Thomas Hobbes, l'indiscusso campione. Come si legge nel XXVI capitolo del *Leviatano*, vero è che "la legge di natura e la legge civile si contengono reciprocamente e sono di pari estensione", per cui sembrerebbe quasi che il filosofo inglese ammicchi alla tradizione d'Info1 o ICR. Ma, prosegue il passo, sono propriamente leggi solo quelle che il potere costituito ha stabilito come tali: "dal fatto che la legge è un comando, e che un comando consiste in una dichiarazione o manifestazione della volontà di colui che comanda – mediante voce, scrittura o qualche altro sicuro segno della medesima volontà – si può comprendere che il comando dello Stato è legge solamente per coloro che hanno i mezzi per prenderne cognizione" (Hobbes ed. 1992: 223-224).

In terzo luogo, infine, bisogna fare i conti con l'"informazione sulla realtà" – ISR o Info3. In questo caso, l'informazione semantica ci informa sui diversi stati del mondo, come quando chiediamo gli orari in cui la segreteria dell'università risulta aperta, o quali siano stati i responsi di una visita medica. Questo tipo d'informazione è qualificabile in senso aletico, ossia, con parole più povere, è definibile come vera o falsa. Per i giuristi, Info3 entra in gioco a più livelli: ora, in senso dottrinale, con gli studi di sociologia del diritto e certe varianti del realismo giuridico; ora, in senso probatorio, con le discussioni di fatto in istruttoria che chiamano, spesso, in causa le consulenze dei periti; ora, in senso pratico, ogni qualvolta il lettore si sia trovato nella necessità di chiedere il parere di un esperto e, entrando nello studio di un avvocato, spera ardentemente che quanto gli è stato detto corrisponda al vero!

Come ben si vede, i diversi modi o livelli secondo cui la nozione d'informazione può essere legittimamente intesa, non soltanto riconducono a quella pluralità, per certi versi disorientante, dei diversi modi in cui il diritto può a sua volta essere rappresentato: si v. sopra §§ 1.1.2 e 1.1.3. In realtà, quanto ancora rimane in sospeso è in che modo tale informazione vada colta come più o meno complessa.

Per venire a capo di questo duplice ordine di questioni, viene in soccorso un'altra volta l'idea di "profondità logica" introdotta all'inizio del presente capitolo. Si tratta, come detto, della nozione che Lloyd ha ripreso dagli studi di Bennett e, prima ancora, di Solomonoff e, soprattutto, di Chaitin. A continuazione (§ 2.1.1), ci soffermeremo pertanto sull'opera di Chaitin, al fine di capire come le nozioni di complessità e informazione possano essere collegate tra di loro. Dopo di che, in § 2.1.2, bisognerà

approfondire come tale concetto di complessità si applichi al mondo del diritto come informazione. Avendo presente le varianti offerte dall'Info1 del giusnaturalismo, dall'Info2 del giuspositivismo, e dall'Info3 della sociologia del diritto e di alcuni tipi di realismo giuridico, occorrerà dar conto di questa molteplicità di prospettive in § 2.1.3. Traendo spunto dall'opera di Chaitin, l'intento è di tracciare, all'insegna dell'"incompletezza", un parallelismo tra il mondo della matematica e l'esperienza giuridica. Lungi dal dar luogo a derive nichilistiche, il terreno sarà pronto per esplorare un nuovo settore del diritto, dinamico e vitale (§ 2.2). Non è forse la complessità la scienza della sorpresa?

### 2.1.1. *Il teorema di Chaitin*

La relazione che Chaitin instaura tra complessità e informazione va intesa alla luce dei suoi studi in tema di casualità che, a loro volta, riconducono ai risultati, per molti versi sensazionali e sconvolgenti, del grande logico-matematico Kurt Gödel (1906-1978), nonché del già ricordato matematico inglese Alan Turing (§ 1.4). Senza entrare nei dettagli, particolarmente ostici, delle relative dimostrazioni, è sufficiente ricordare, nel caso di Gödel, come il suo genio sia consistito nel tradurre nel linguaggio della meta-matematica una proposizione vera che, tuttavia, affermi di sé di non essere dimostrabile all'interno del sistema logico di riferimento. Come nel classico paradosso del mentitore cretese, davanti alla proposizione "io dico il falso", essa è vera, o falsa? Infatti, qualora volessimo dimostrare la verità di una proposizione che sappiamo essere indimostrabile, staremmo provando per ciò stesso il falso: cosa che, ammetterete, nessun matematico al mondo amerebbe fare. Ma allora, per non dimostrare una falsità, bisogna giungere alla conclusione che, per salvare la coerenza del sistema, quest'ultimo debba essere per forza incompleto. Anche supponendo di sopperire all'incompletezza del sistema con l'aggiunta di nuovi assiomi, il devastante risultato di Gödel è che non otterremo mai un sistema completo, dato che avremo sempre a che fare con verità che sappiamo essere tali e che, nondimeno, non possono essere dimostrate all'interno del sistema considerato.

Nel caso di Turing, egli è partito dal problema di escogitare un algoritmo, vale a dire le procedure di calcolo, con le quali dar conto di tutte le domande possibili della matematica. Muovendo dal più semplice e familiare algoritmo – quello delle operazioni di addizione e moltiplicazione dei numeri naturali: 0, 1, 2, 3… – occorre computare tutta la ricchezza relativa alle proposizioni teoretiche nella teoria dei numeri con l'addizione e la moltiplicazione. A questo scopo, nel memorabile scritto del 1937 *Sui numeri computabili*, Turing immaginò una "macchina calcolatrice" a circuiti elettrici, in grado di fare tutto ciò che può essere calcolato con un algoritmo. A questo fine, egli escogitò il modello matematico di una macchina calcolatrice onnifunzionale capace di fare, senza aiuti dall'esterno, tutto ciò che può essere calcolato da una qualsiasi "macchina di Turing". Definito come insieme di arresto l'insieme dei numeri delle macchine destinate ad arrestarsi una volta trovata una risposta al problema sollevato, a differenza delle macchine che possono procedere nel calcolo all'infinito, il risultato ottenuto da Turing era ancora una volta sorprendente. Non esiste, infatti, un algoritmo per decidere una volta per tutte se la condizione d'arresto del programma sarà mai raggiunta poiché, stante lo stesso teorema di incomple-

tezza di Gödel, esiste necessariamente un insieme diverso dall'insieme di arresto di qualsiasi macchina di Turing. D'un colpo solo, il matematico inglese poneva non soltanto le basi logico-matematiche degli odierni computer ma, come se non bastasse, dimostrava ciò che nessun computer al mondo potrà mai calcolare!

Il passo successivo lungo questo filone di ricerca conduce al teorema di Chaitin: uno dei meriti della sua opera consiste infatti nell'aver reso, per così dire, naturali i risultati ottenuti da Gödel e Turing, formalizzando una serie di problemi matematici per la cui soluzione è richiesta più informazione di quella contenuta nella stessa domanda. Da un lato, Chaitin approfondisce un aspetto dei teoremi di Gödel, e cioè quello relativo all'indecidibilità relativa a una sequenza, o lista di numeri, la cui lunghezza, o complessità, sia maggiore di quella del programma informatico che deve stabilire se tale sequenza è casuale. D'altro canto, a differenza di Turing, Chaitin non considera un solo programma alla volta ma, insieme, tutti i programmi possibili, scegliendone uno a caso e chiedendo quale sia la probabilità che questo programma scelto a caso, si arresti. Il risultato è quanto Chaitin stessa chiama il "gioiello della corona" della teoria algoritmica dell'informazione. Sommando per ogni programma che si arresta, la probabilità di avere precisamente quel programma scelto a caso, avremo la "probabilità d'arresto omega":

$$\Omega = \sum_{\text{programma p che si arresta}} 1/2^{\text{numero di } \textit{bits} \text{ in p}}$$

Rinviamo il lettore curioso dei dettagli tecnici ai volumi della presente collana che si sono soffermati sul punto (Pagallo 2005; Chaitin 2006; Lolli e Pagallo 2008).

Qui, è sufficiente notare che i valori decimali di Ω non sono deducibili da altri fatti e assiomi matematici, né tali valori possono essere calcolati da un computer. Piuttosto, è come se occorresse lanciare in aria una moneta (non truccata, specialmente in Italia), per stabilire a posteriori in chiave binaria, se testa 0, se croce 1:

$$\Omega = 0{,}0010010101001011010\ldots$$

Ciascuna cifra binaria di Ω è del tutto indipendente dalle altre dal punto di vista logico, ed è vera per nessuna ragione: Ω è infatti un numero del tutto casuale. Ciò che comporta che se, come affermava il padre della relatività, Albert Einstein (1879-1955), "Dio non gioca a dadi", bisogna pure arrendersi all'evidenza e ammettere che, almeno nel campo della matematica, se la divinità esiste, allora gioca a dadi!

Tirando le fila del discorso, quale dunque il nesso tra complessità e informazione?

In sintesi, si può che dire che il nesso tra i due concetti è dato dalla nozione di comprimibilità teorica, per cui, maggiore la complessità dell'oggetto di studio, maggiore la quantità dell'informazione necessaria per rappresentare tale oggetto, perché minore il grado della sua comprimibilità teorica. Viceversa, maggiore la compressione raggiungibile dalla teoria, minore la quantità delle informazioni necessarie, minore la sua complessità. Nel caso specifico di Ω, abbiamo pertanto a che fare con un numero che, per dirla con il titolo di un articolo apparso nel giugno 1988 su *The Los Angeles Times*, ha fatto "tremare un po' il mondo", perché non c'è modo di rappresentarlo, se non riproducendolo tale e quale. Zero ridondanza, massima complessità.

È tempo di esaminare il modo in cui questi risultati della meta-matematica possano essere mai rilevanti nel campo del diritto.

### 2.1.2. *Il diritto come informazione*

Ci sono due modi – uno elementare, l'altro sofisticato – per cogliere l'importanza dei risultati di Chaitin nell'ambito giuridico. Muovendo dal semplice al complesso, tali risultati si colgono innanzitutto sul piano IPR-Info2 del § 2.1, vale a dire sul piano della informazione giuridica come insieme di regole che determinano il modo di essere di altre entità. Per orientare il lettore, sarà opportuno mostrare a che punto siamo della nostra analisi con una nuova figura. Essa illustra non soltanto i tre noti osservabili della figura 5, ma introduce altresì le tre variabili di IPR:

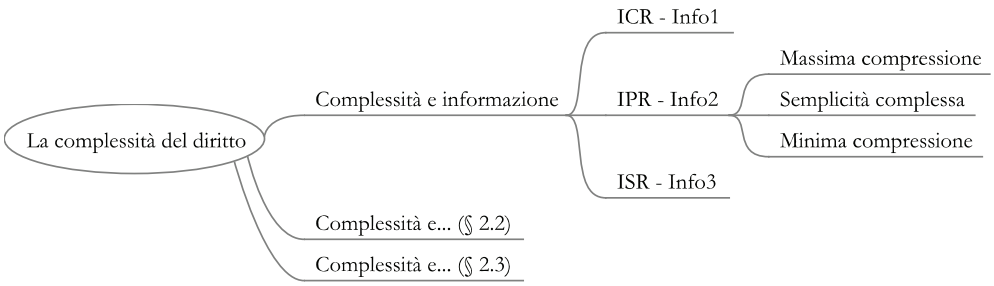


Figura 6: *Lo spettro dell'informazione giuridica per la realtà*

Come riferito in precedenza (§ 1.4.1), a proposito dell'informatica giuridica detta "decisionale", una prima convergenza tra matematica e diritto è data dalla legittimità di concepire la legge alla stregua di un algoritmo. Definito quest'ultimo come un'operazione matematica o "un metodo di risoluzione che, operando sui dati predetti con relazioni logiche e/o di calcolo, permette di ottenere il risultato voluto" (Borruso e Tiberi 2001: 248), ci si è chiesto retoricamente se la stessa definizione non valga anche per il diritto come IPR. Con le parole di uno dei pionieri italiani dell'informatica giuridica, nonché presidente aggiunto onorario della Corte di cassazione, "la definizione dell'algoritmo non coincide, infatti, con la definizione della legge? Non è forse anche la legge un complesso di regole generali e astratte, formulabili *ex ante*?" (Borruso 1997: 658).

Su queste basi, è dato delineare il seguente spettro. Ad un estremo, secondo gli auspici di Borruso, troviamo le leggi generali ed astratte per le quali vale il massimo della compressione informativa ottenibile con un algoritmo che, come proprio risultato, diminuisce la complessità del diritto tramite leggi chiare e precise. All'estremo opposto, troviamo invece le cosiddette leggi "ad personam" in cui la compressione, va da sé, è minima, trattandosi di provvedimenti particolari e concreti. Come esempi di ciò che possiamo compendiare, per una volta in inglese, come "one man, one law", valgano, tra le tante, le sentenze che la Corte costituzionale ha dovuto pronunciare nel 2004 (n. 13 avverso la legge 140 del 2003, il cosiddetto "lodo Schifa-

ni"); nel 2007 (n. 26 avverso la legge 46 del 2006 o "legge Pecorella"); e nel 2009 (n. 262 avverso la legge 124 del 2008 o "lodo Alfano").

A metà strada tra i due estremi, va collocata la classe di leggi apparentemente semplici che, nondimeno, danno luogo a casi complessi e, cioè, casi che richiedono dosi crescenti di informazione per essere convenientemente istruiti e, possibilmente, risolti. Tra le tante ragioni, si pensi all'uso da parte del legislatore di clausole generali, come le nozioni di "buona fede", o "buon padre di famiglia"; la necessaria contestualizzazione dei concetti in gioco, come "dato personale" o "controllore dei dati"; oppure il riscontro fattuale delle ipotesi previste dalla legge, come nel caso delle perizie o delle consulenze tecniche d'ufficio.

Ma, senza entrare nel dettaglio, non sfugga un elemento essenziale: ciò che va opposto al "complesso" non è quanto è "semplice", bensì il "determinato". Come illustrato dal numero Ω di Chaitin, possiamo avere una definizione chiara e precisa della legge, senza che questo di per sé prevenga la scarsa (o nulla) comprimibilità teorica delle informazioni necessarie per la rappresentazione dell'oggetto di studio. Da questo punto di vista, ne consegue un'ulteriore ragione di critica a quelle già mosse in precedenza alle tesi del tecno-determinismo: v. § 1.2. Infatti, seguendo queste ultime tesi, sfuggirebbe una ragione fondamentale grazie alla quale l'impatto della rivoluzione tecnologica ha contributo a creare l'odierna società complessa!

Tuttavia, esiste un ulteriore e più sofisticato motivo per cui i risultati di Chaitin sono interessanti per l'analisi del fenomeno giuridico. Questa ragione, se da un lato ci riconduce ai fenomeni di incompletezza rilevati nel paragrafo precedente, d'altro canto richiede una breve digressione sul perché l'analisi del diritto e delle sue convergenze con gli studi della matematica non investa soltanto il livello d'astrazione IPR – Info2. Del resto, vale la pena di aprire questa breve parentesi, dato che avremo occasione di approfondire la conoscenza di colui che abbiamo già presentato come padre della scienza giuridica e politica moderna, vale a dire Thomas Hobbes.

### 2.1.2.1. *Il giuspositivismo di Hobbes*

Hobbes è un pensatore complesso e affascinante. Egli rappresenta per così dire lo snodo che conduce dall'antico al moderno, dal classico al contemporaneo, allo stesso modo in cui abbiamo apprezzato Platone come una sorta d'interfaccia tra due mondi: dall'era dell'oralità a quella della scrittura.

È tipico di Hobbes riprendere i concetti chiave della tradizione, per modificare il loro significato: come esempio, si prenda la nozione di libertà. Per i classici, come il Platone de *La Repubblica*, la libertà va intesa come auto-disciplina, in ragione del fatto che la parte migliore di noi stessi ha il sopravvento su quella peggiore, governandola: un eco di questa antica concezione permane ancora ai nostri giorni, quando si sente dire che un malato di mente o un tossicodipendente non è più padrone di sé. Viceversa, per Hobbes, la libertà del soggetto va intesa come assenza d'impedimenti esterni e, cioè, più semplicemente, come la capacità di fare ciò che si vuole: in fondo, il lettore si accorgerà di essere spesso un nipotino di Hobbes senza saperlo!

Ma, l'osservazione vale ancor più in generale per le nozioni di diritto e legge naturale: Hobbes viene non di rado annoverato tra gli esponenti del giusnaturalismo moderno – ICR o Info1 nel nostro gergo. E, infatti, nelle sue grandi opere

come il *Leviatano* o il *De Cive* (sul cittadino), Hobbes dedica interi capitoli al concetto di stato di natura, alla legge di natura fondamentale, ossia al dovere di cercare la pace, oltre a numerose altre leggi di natura in tema di giustizia, gratitudine, reciproca disponibilità, facilità a perdonare, e via dicendo. Tuttavia, Hobbes è anche giustamente famoso per aver compendiato i rapporti che si danno in questo stato di natura, con la formula dell'antico comico romano Plauto, come uno stato di guerra: "homo homini lupus". Questa condizione, che dipende dal fatto che le leggi di natura, in realtà, vincolano soltanto in foro interno, significa che allo stato di natura ciascuno pretende di aver diritto a tutto, contro tutti. Non si tratta peraltro di una semplice supposizione filosofica: a giudizio di Hobbes, questo stato si verifica concretamente nell'occasione di ogni guerra civile e, lasciando da parte il suo giudizio sugli indiani d'America, nelle relazioni internazionali, diremmo noi oggi, tra stati sovrani. Quanto questo nuovo modo di intendere l'allora diritto pubblico europeo abbia inciso nella pratica degli stati, lo si dirà in un secondo momento; ma, per dare fin d'ora conto del peso esercitato dalle idee di Hobbes, basti riferire che la concezione delle relazioni internazionali basate sulla legge del più forte ha trovato grande fortuna anche tra i più recenti presidenti degli Stati Uniti d'America. Per illustrare il punto, non serve l'esempio, fin troppo facile, di George W. Bush e la sua invasione dell'Iraq nel 2003, la cosiddetta seconda guerra del golfo. Piuttosto, è sufficiente riportare un passo del discorso tenuto dal presidente democratico Bill Clinton davanti alle Nazioni Unite il 27 settembre 1993, in cui rivendicava il diritto del suo paese "all'uso unilaterale della forza militare [per] assicurare l'accesso ai mercati chiave, risorse energetiche e strategiche". Siamo proprio nipotini di Hobbes!

Nondimeno, come fuoriuscire da questo stato di guerra, almeno sul piano interno della propria nazione?

La risposta, ancora una volta classica, di Hobbes è mediante un contratto sociale. Lasciando da parte le oscillazioni che Hobbes ha avuto al riguardo, tra il concetto di rappresentanza e autorizzazione nel *Leviatano*, e l'idea di trasferimento a uno solo del diritto di tutti nel *De Cive*, si può dire che il contratto sociale di Hobbes appare come un atto di rinuncia unilaterale in favore di un terzo, che non prende parte a quel contratto, vale a dire il "sovrano". Per garantire la fondamentale legge di natura che prescrive di cercare la pace, in altri termini, ciascun individuo deve rinunciare alla propria pretesa di avere diritto su tutto contro tutti, tipica dello stato di natura, per cui l'unico diritto che può alla fine dirsi propriamente tale, non può che essere ciò che il sovrano vorrà nella società civile. Muovendo da premesse classiche di diritto naturale, Hobbes getta le basi della tradizione a venire, e cioè il giuspositivismo moderno: da ICR o Info1 a IPR o Info2, come unica sensata prospettiva, o livello d'astrazione, da cui dar conto del diritto.

Questa variante assolutistica del contratto sociale, per cui non ci sono limiti di diritto alla volontà del sovrano, per ciò stesso sciolto dalle leggi (*legibus solutus*), trova però una serie di vincoli, o vere e proprie contraddizioni nel pensiero di Hobbes. Ne segnalo tre: in primo luogo, si tratta della causa del contratto e, cioè, della ragione per la quale con tale contratto si è rinunciato ai propri diritti; avere salva la vita. Dal punto di vista della causa del contratto, sembrerebbe che, nel caso in cui il suddito rischia la propria vita per via di una decisione del sovrano, il con-

tratto debba ritenersi per ciò sciolto. Questa interpretazione viene tuttavia respinta a più riprese nel *Leviatano*, sulla base della tesi che la clausola con la quale il suddito rinuncia ai propri diritti mediante il contratto sociale, autorizza il sovrano a rappresentarlo; e pertanto, anche nel caso in cui il suddito sia condannato a morte, dovremmo concludere che si è trattato di una sorta di suicidio! Sempre nel *Leviatano*, capitolo ventunesimo, questa tesi pare nondimeno contraddetta dall'altra affermazione, per cui "quando il nostro rifiuto di obbedire vanifica il fine per il quale è stata istituita la sovranità, allora non c'è alcuna libertà di rifiutare [l'obbedienza], in caso contrario [questa libertà] c'è" (Hobbes ed. 1992: 182). Al riguardo, è significativo che molte delle critiche e polemiche sorte ai tempi della pubblicazione del *Leviatano*, siano giunte a Hobbes, come diremmo oggi, da destra, più che da sinistra: basti dire che il vescovo John Bramhall, recensendo il lavoro di Hobbes in *The Catching of the Leviathan* del 1658, liquidò l'opera come "il catechismo del ribelle".

In secondo luogo, nonostante l'indubbio assolutismo di Hobbes, egli deve pur sempre ritenersi precursore del principio di legalità. Come ricordato più sopra (§ 1.2), è pur vero che la legge è quanto stabilisce il sovrano con la sua volontà, per cui, in caso di dubbio, l'ultima parola che conta è quella dell'interpretazione autentica del sovrano e non certo quella dei giudici. Ma, come detto, questa legge è tale a una condizione, e cioè che il sovrano l'abbia resa pubblica "mediante voce, scrittura o qualche altro sicuro segno della medesima volontà". Sotto questo aspetto, Hobbes è certamente precursore, in funzione garantista, del diritto come informazione.

In terzo luogo, infine, il costrutto giuspositivistico al quale aspira Hobbes è dato dal rigore del metodo geometrico che, però, sempre nel capitolo ventunesimo del *Leviatano*, sembra revocato in dubbio dallo stesso filosofo, quando ammette che "sebbene la sovranità, nelle intenzioni di coloro che la istituiscono, sia immortale, tuttavia, per sua natura non solo è soggetta a morte violenta a causa della guerra contro nemici esterni, ma anche reca in sé, fin dalla stessa istituzione […] i molti semi della mortalità naturale generati dalla discordia intestina" (*op. cit.*, 185). Come risultato, non soltanto dobbiamo riconoscere che "l'obbligazione dei sudditi verso il sovrano è intesa durare fintantoché – e non più di quanto – dura il potere con cui quegli è in grado di proteggerli" (p. 184). In realtà, con buona pace del giuspositivismo, questo significa che bisogna distogliere l'attenzione dal livello di astrazione definito da IPR o Info2, per concentrarci intanto su ISR-Info3, vale a dire sull'informazione fattuale circa l'effettività o meno del potere del sovrano; e, poi, far ritorno a ICR-Info1, per stabilire quale sia il senso di questo sorgere e perire di poteri costituiti.

### 2.1.2.2. *Il diritto come informazione (segue)*

Dopo i brevi cenni al pensiero di Hobbes, l'impressione è di essere approdati in una sorta di paradosso o, peggio ancora, di vicolo cieco, poiché ci ritroviamo a dover fare i conti con quella molteplicità di vedute sulla natura del fenomeno giuridico che, sin dal § 1.1.2, avevo dichiarato di voler tralasciare. Il quadro generale è riassunto da una nuova figura che riconduce da IPR o Info2, a ICR o Info1:

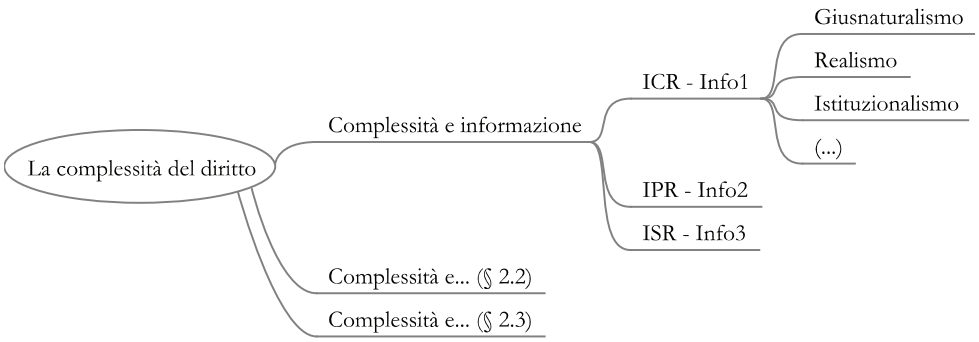


Figura 7: *Il dissidio filosofico sull'informazione giuridica come realtà*

Da un lato, abbiamo infatti riferito come, seguendo il pensiero di Hobbes, si passi da Info2 a Info1, transitando per Info3, per cui ci si può chiedere se la visione del diritto, fondato sull'effettività del potere sovrano, non fa altro che ricondurre alle vecchie tesi del sofista Trasimaco nella *Repubblica* di Platone, ossia al diritto come espressione del potere del più forte. D'altro canto, si può assumere il livello d'astrazione del diritto come informazione senza accogliere quest'ultima conclusione e, anzi, adottando ora posizioni giusnaturalistiche, ora quantomeno pluralistiche, in contrasto, cioè, con il monismo hobbesiano della volontà del sovrano come unica fonte normativa del sistema. Come esempio, basterebbe ricordare le tesi del mio predecessore alla cattedra di Torino, Enrico di Robilant (1924-2012), il quale non soltanto rappresentava il diritto in chiave, appunto, di sistemi informativo-normativi ma, avendo di mira i problemi specifici della complessità nell'età industriale, insisteva proprio sulla pluralità dei centri d'informazione normativa: "nella società industriale, infatti, oltre alla normazione emanante dal potere politico, quella normazione, cioè, a cui comunemente la scienza giuridica riserva la sua attenzione, opera, e ha importanza non minore, e talvolta maggiore, la normazione emanante dai centri di potere economico, sociale e d'informazione, grandi o piccoli che siano" (di Robilant 1973: 227).

Più tardi, nel quarto capitolo in tema di fonti, avremo occasione di tornare sulle intuizioni de *Il diritto nella società industriale*: ma, tornando al nostro paradosso, dovremmo pur aggiungere alla lista dei modi filosofici secondo cui è stata intesa l'informazione del diritto come sistema complesso, altre e diverse scuole. Si pensi al realismo giuridico, oppure all'istituzionalismo, secondo cui, anche ad adottare la visione realista del "dio mortale" hobbesiano, l'idea di fondo è che i sovrani passino ma le istituzioni restino.

Come, dunque, venire a capo di questa molteplicità di vedute?

È qui che entra in gioco il modo sofisticato d'intendere l'importanza dei risultati ottenuti da Chaitin nell'ambito della meta-matematica per lo studio filosofico dei giuristi.

### 2.1.3. *Fenomeni d'incompletezza*

La ragione per la quale le ricerche di Chaitin hanno reso del tutto naturali i pur sconvolgenti risultati di Gödel e Turing, a proposito d'indecidibilità, incompletezza e non computabilità, dipende dal fatto che Chaitin ha mostrato come la verità (matematica) vada intesa come sotto-insieme della complessità. Sappiamo infatti che un'infinita parte delle verità matematiche sono destinate a rimanerci ignote per sempre. Questo corollario dei teoremi di Gödel, com'è comprensibile, ha provocato un vivace dibattito tra logici, matematici e, in genere, i filosofi della conoscenza, sulle possibili derive nichilistiche che discendono da detti teoremi. Basti pensare in modo approfondito al teorema di Tarski (1901-1983), sull'indefinibilità della verità, per cui "parlare di verità matematiche è inevitabilmente condannato alla vaghezza, se il linguaggio è informale, oppure al rinvio indefinito a metalinguaggi rigorosi sempre più problematici […] Ogni realista dovrebbe appendersi davanti al posto di studio un cartello con la scritta *Memento Tarski*" (Lolli 2002: 80-81).

Un'ulteriore maniera per chiarire la questione, consiste nel dire che i fenomeni d'incompletezza e affini dipendono dal fatto che il mondo della matematica, in realtà, è più complesso del suo stesso linguaggio. Per quanto s'intenda sopperire all'incompletezza dei sistemi formali aggiungendo nuovi assiomi, non soltanto la coerenza di tali sistemi non potrà essere dimostrata al loro interno, ma rimarranno sempre alcune proposizioni che saranno indecidibili. Allo stesso modo, per quanto si aumenti la potenza di calcolo dei computer, essi saranno in grado di determinare soltanto una parte finita dell'infinita complessità necessaria per determinare i valori di Ω. Lasciando impregiudicato il mai superato dibattito sul parallelismo tra matematica e diritto, l'insegnamento che possiamo trarre dalle ricerche di Chaitin è dunque duplice. In primo luogo, le limitazioni che discendono dai fenomeni d'incompletezza valgono anche per il linguaggio che ha di mira il mondo del diritto: le varie scuole giusnaturalistiche, giuspositivistiche, istituzionalistiche, realistiche, ecc., possono infatti cogliere questo o quell'aspetto del fenomeno giuridico, ma non certamente darne conto nella sua interezza. Per dirla con Friedrich Hayek, "dubito che qualcuno sia mai riuscito a verbalizzare tutte le regole che costituiscono il 'fair play'" (Hayek 1986: 99).

In secondo luogo, nel dichiarare che il mondo del diritto è più complesso del suo linguaggio, non si vogliono avvalorare derive nichilistiche e, cioè, il fatto che ciascuno possa dire ciò che vuole: in fondo, ciò non accade nemmeno ai matematici eredi di Gödel o di Chaitin! Piuttosto, nel comprendere le ragioni delle molteplici prospettive in cui il fenomeno del diritto è assunto come ICR-Info1, IPR-Info2, o ISR-Info3, la dose d'umiltà che l'incompletezza suggerisce, consiglia di tornare all'insegnamento aristotelico (v. sopra § 1.1.1). Trattandosi di un sapere che non è fine a sé ma, bensì, di un sapere per fare, come mezzo per l'azione, occorre andare oltre al sapere dei giuristi e dei filosofi di professione, per fare attenzione al diritto come pratica sociale e a ciò che possiamo apprendere dalla interazione dei soggetti. È precisamente su questo tema che s'incentra il paragrafo che segue.

## 2.2. *Le forme dell'emergenza*

Il secondo osservabile dell'indagine sul diritto, tra complessità e informazione, concerne la nozione di "emergenza". Come suggeriscono svariate lingue, come l'inglese, che distingue tra "emergency" ed "emergence", bisogna tenere separate due accezioni del lemma. Nel caso dell'emergenza come *emergency*, si tratta dell'ipotesi più familiare al lettore italiano, trattandosi di emergenza come stato di crisi e urgenza, cui corrispondono di solito poteri straordinari. Forse la più nota (e discutibile) definizione al riguardo è quella del giurista tedesco Carl Schmitt (1888-1985), secondo il quale "sovrano è colui il quale decide dello stato di eccezione". Siccome, però, questa prima accezione ci ricondurrebbe al livello d'astrazione d'IPR-Info2, possiamo tralasciarla in questa sede.

Nel caso dell'emergenza come *emergence*, invece, il riferimento va alle forme in cui gli ordini giuridici emergono, appunto, dalla complessità dell'esperienza. Tra le forme tradizionali secondo cui i giuristi hanno mirato a catturare il fenomeno, si pensi sin d'ora agli usi e alle consuetudini, fonti del diritto che non dipendono da un atto di volontà ma, piuttosto, rinviano all'interazione spontanea dei soggetti. In termini più generali, questa forma d'emergenza si ritrova nella distinzione, ancor oggi popolare, tra ordinamenti giuridici consuetudinari, come il *common law* inglese, e gli ordinamenti di *civil law* del continente europeo. In termini filosofici, questa distinzione è stata ulteriormente raffinata dal ricordato economista viennese Friedrich Hayek, nella sua opera di filosofia del diritto *La società libera* (1960; tr. it. 1999); e, soprattutto, nei tre volumi di *Legge, legislazione e libertà* (1973-1979; tr. it. 1986).

Da un lato, Hayek riassume con il termine di "taxis" tutte le tradizionali fonti atto dell'ordinamento, ossia la legislazione e ogni forma di costruttivismo politico. Trattandosi dell'insieme delle regole volte a determinare il modo di essere di altre entità nel diritto, tralasciamo, come detto, il ruolo che la *taxis* come IPR-Info 2 svolge in questa sede.

D'altro canto, Hayek designa come "kosmos" le fonti fatto del diritto, vale a dire le forme di emersione degli ordini spontanei come la consuetudine e gli usi. A differenza della *taxis*, dove il diritto può essere convenientemente rappresentato come frutto della progettualità politica degli uomini, della loro volontà, il diritto come *kosmos* va invece colto all'interno del percorso evolutivo della nostra specie.

Riportando questa distinzione ai temi della complessità e del diritto come sistema informativo, la differenza tra *taxis* e *kosmos* è cruciale. Con le parole di Hayek, "gli ordini spontanei non sono necessariamente complessi, ma a differenza delle deliberate sistemazioni umane, essi possono possedere qualsiasi grado di complessità. Una delle principali tesi che cercheremo di dimostrare sarà che gli ordini molto complessi, che comprendono più fatti particolari di quelli che qualunque cervello è in grado di accertare e manipolare, possono essere raggiunti solo mediante il gioco delle forze che portano alla formazione degli ordini spontanei" (Hayek ed. 1986: 53).

Su queste basi, possiamo approfondire il secondo osservabile dell'analisi con due variabili, come illustrato dalla seguente figura:

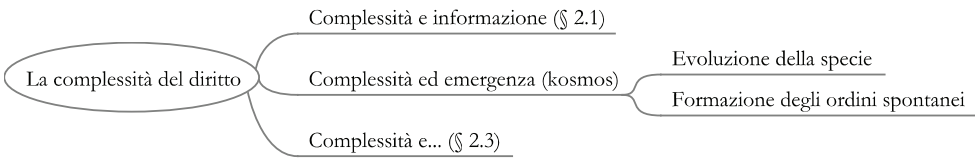


Figura 8: *Emergenza, evoluzione e ordini spontanei*

A continuazione, in § 2.2.1, l'attenzione sarà incentrata sulla prima variabile del secondo osservabile della figura 8: riprendendo l'approccio evolutivo di Hayek, avremo modo di approfondire le avventure dell'*homo technologicus* introdotte nel § 1.1.

Dopo di che, in § 2.2.2, vedremo come si formano gli ordini spontanei, facendo ricorso alla metodologia della teoria delle reti. Questa prospettiva consentirà di mettere a fuoco alcuni dei più affascinanti fenomeni d'ordine spontaneo emersi negli ultimi tempi, vale a dire i "mondi piccoli" d'internet (§ 2.2.2.1). Non è forse sempre la complessità la scienza della sorpresa?

### 2.2.1. *L'evoluzione cosmica di Hayek*

Per cogliere la nozione hayekiana di evoluzione cosmica, la questione preliminare da affrontare è quella della sopravvivenza e adattamento della specie all'ambiente. Al pari delle considerazioni che Socrate sviluppa nella *Repubblica* a proposito della *polis* primitiva (v. § 1.1), ogni organizzazione volta a questo fine essenziale – attraverso la divisione del lavoro, il mercato, la moneta … – è il risultato di un percorso evolutivo che seleziona le strategie di adattamento. "Pertanto la società può esistere solo se, mediante un processo di selezione, si sono evolute delle regole che conducono gli individui a comportarsi in modo tale da rendere possibile la vita sociale" (Hayek 1986: 59). In ragione di questo processo evolutivo, la società "nel breve spazio di meno di ottomila anni" è venuta progredendo dalle comunità di nomadi cacciatori agli agricoltori, fino alla vita cittadina vera e propria, la cui realizzazione è iniziata "forse meno di tremila anni o di cento generazioni fa" (*op. cit.*, 74). Le regole mediante le quali gli uomini hanno imparato ad adattarsi al proprio ambiente, non dipendono perciò da una volontà o progetto consapevole: piuttosto, le norme si presentano innanzitutto come il prodotto spontaneo, ossia non programmato, dell'interazione umana. Da questo punto di vista, "la posizione sostenuta in questo libro sarà quindi presentata probabilmente dai positivisti come una teoria del diritto naturale" (Hayek 1986: 258).

Questa particolare dimensione spontanea dell'esperienza trova conferma nella natura dinamica ed evolutiva della mente umana. Per dirla ancora con il nostro filosofo, "la mente è il risultato di un adattamento all'ambiente naturale e sociale in cui l'uomo vive, e che si è sviluppata in costante interazione con le istituzioni che determinano la struttura della società. La mente è tanto un prodotto dell'ambiente sociale in cui è avvenuta la sua crescita, quanto qualcosa che a sua volta ha influenzato e modificato le istituzioni della società" (*op. cit.*, 25). Concependo l'esercizio dell'in-

telligenza e della comprensione come sistemi che mutano di continuo, come risposte alle sfide e alle sollecitazioni dell'ambiente – per cui alcuni modi di agire prevalgono sugli altri in ragione del loro maggiore successo – la conseguenza è che l'ordine dell'interazione tra gli individui non è il risultato cui giunge l'intelligenza teorica umana, essendo piuttosto la condizione dello sviluppo della mente medesima: "L'uomo non ha adottato nuove regole di condotta perché era intelligente. È diventato intelligente sottomettendosi a nuove regole di condotta" (Hayek 1986: 542).

In opposizione alle visioni costruttivistiche delle istituzioni che fanno leva sulla volontà e progettualità umana, Hayek insiste sul fatto che, attraverso il consolidamento dei costumi e delle consuetudini – come conferma il caso dell'economia, con il mercato o la moneta – anche il diritto sorge come fenomeno originariamente spontaneo e, cioè, non intenzionale. La successiva teorizzazione delle regole che hanno consentito agli uomini di adattarsi all'ambiente naturale e sociale, non deve in altri termini far dimenticare che l'ordine spontaneo rappresenta la condizione primaria per la istituzionalizzazione delle relazioni tra gli individui. Ancora una volta con le sue parole, "la storia del diritto propriamente detta inizia ad uno stadio troppo avanzato dell'evoluzione per gettare luce sulle origini […] Gli individui hanno imparato ad osservare (e a sanzionare) regole di condotta molto prima che tali regole potessero venir espresse in forma verbale" (Hayek 1986: 96).

Al pari dei più illustri esponenti della tradizione classica del diritto naturale, come Platone o Aristotele, l'intento di Hayek non è stato tuttavia quello di negare che il diritto sia anche il prodotto della volontà dell'uomo. A più riprese in *Legge, legislazione e libertà*, egli ammette l'esistenza di "due modi in cui un ordine può avere origine" (*op. cit.*, 50); e, anzi, che quel tipo di organizzazione chiamato "governo" sia indispensabile alla società (*op. cit.*, 62-63).

Nondimeno, la tesi che Hayek difende è che, nonostante le apparenze, gli ordini posti in essere scientemente dal legislatore, secondo il modello costruttivistico messo a punto a partire dalla filosofia giuridica di Hobbes, danno luogo a ordini relativamente semplici o con "moderati gradi di complessità". La mente umana è infatti capace di fronteggiare soltanto una piccola parte dell'informazione richiesta per disciplinare l'interazione sociale. L'ordine che emerge spontaneamente con il *kosmos*, le consuetudini o gli scambi economici, è perciò assai più complesso di quanto l'uomo riesca a calcolare o a gestire artificialmente, poiché "il suo grado di complessità non è limitato da quanto la mente umana è in grado di padroneggiare" (Hayek 1986: 53).

Si tratta pertanto di indagare a continuazione come sorgano, e funzionino, tali ordini spontanei.

### 2.2.2. *La formazione degli ordini spontanei*

Gli esempi d'ordine spontaneo sui quali ha attratto l'attenzione Hayek sono quelli classici delle consuetudini giuridiche e del mercato economico con le loro interdipendenze, secondo ciò che gli è valso del resto il Nobel nel 1974. Da un punto di vista giuridico, il richiamo alle consuetudini solleva tuttavia un duplice ordine di problemi: innanzitutto, viene spesso ammesso che le consuetudini rappresentino la fonte primigenia o originaria delle istituzioni che, tuttavia, con l'evolvere del diritto, sarebbe stata soppiantata dalla fonte del diritto legislativo. L'appunto sarebbe con-

fermato dall'esempio del diritto internazionale a base consuetudinaria, fondato cioè sulla seconda legge hobbesiana di natura per cui "bisogna stare ai patti" (*pacta sunt servanda*). Questo fondamento, infatti, proverebbe la natura poco evoluta, o primitiva, dell'odierno diritto internazionale.

Per evitare questo tipo di dibattito, è forse dunque il caso di illustrare le forme hayekiane d'ordine cosmico sulla scorta di un esempio, quello di internet, e di una teoria, quella delle reti, che Hayek, morto a Friburgo nel marzo 1992, non poteva conoscere. È soltanto con l'articolo che Steven Strogatz e Duncan Watts pubblicarono sulla rivista *Nature* nel 1998, che avremmo cominciato a disporre delle opportune lenti concettuali con cui decodificare i nuovi fenomeni del *kosmos*. Di cosa si tratta?

Al riguardo, bisogna per prima cosa cominciare a familiarizzarsi con le categorie elementari della teoria delle reti, vale a dire:

i) i nodi della rete, come suoi elementi costitutivi;
ii) i collegamenti tra i nodi, come mezzo proprio d'interazione;
iii) il diametro della rete, come distanza media tra i nodi.

Su queste basi, illustrate qui sotto dalla figura 9, è possibile delineare tre diversi modelli di rete che prendono in considerazione il fenomeno della casualità cui si è già fatto cenno con le ricerche di Chaitin (§ 2.1.1):

i) reticolo regolare;
ii) reticolo casuale;
iii) reticolo a mondi piccoli.

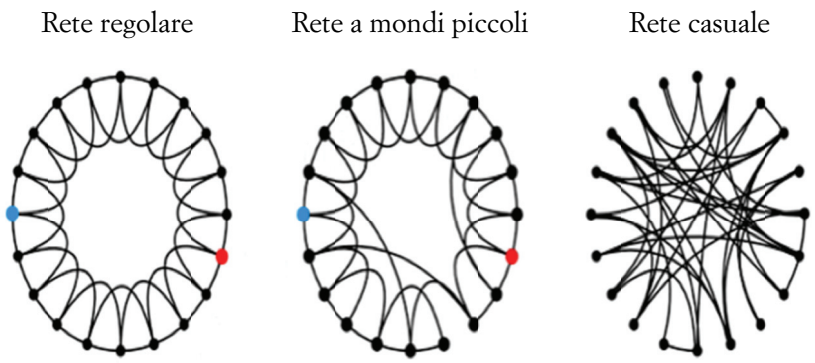


Figura 9: *Tre modelli di rete*

Nella rete regolare, tutti i nodi hanno lo stesso numero di collegamenti: questo reticolo ha un alto coefficiente di raggruppamento ma un diametro lungo, nel senso che il grado di separazione tra i nodi è alto.

Viceversa, nel reticolo casuale il coefficiente di raggruppamento è basso, dato che molti nodi hanno pochi collegamenti e, tuttavia, il diametro si è di molto accor-

ciato. Ciò dipende dai collegamenti a caso nel reticolo, che riducono esponenzialmente il grado di separazione media tra i nodi.

In mezzo a questi due modelli, troviamo la rete a mondi piccoli: la sua peculiarità consiste nel fatto che, come le reti regolari, i mondi piccoli presentano alti coefficienti di raggruppamento; ma, come le reti casuali, hanno un caratteristico diametro accorciato. Ciò significa che i nodi richiedono mediamente pochi passi per raggiungersi a vicenda. Ad esempio, nel reticolo regolare, ci sono 20 nodi, ciascuno dei quali ha 4 collegamenti, per cui il nodo blu (quello più chiaro sulla sinistra) ha bisogno di 5 passi per raggiungere il nodo rosso (quello più chiaro sulla destra). Ciò che è sorprendente con le reti a mondi piccoli è come i collegamenti casuali riducano esponenzialmente il grado di separazione tra i nodi: così, collegando a casaccio solo 3 nodi, il grado di separazione scende da 5 a 3. Questo significa che se immaginiamo il nostro pianeta come un cerchio avente 6 miliardi di nodi/persone, è sufficiente che i collegamenti casuali nella rete siano 2 ogni 10 mila, affinché il grado di separazione media tra i nodi si attesti a 8. Ma se quei collegamenti fossero 3, allora 5!

Tuttavia, rispetto a questo modello (Watts e Strogatz 1998), un suo fondamentale ingrediente venne messo a punto soltanto nel 2002 da Albert-László Barabási: egli infatti notò che nella maggior parte delle reti nel mondo reale, come la rete d'internet, l'aggiunta continua di nodi si dispone secondo una legge di potenza. Ciò significa che la probabilità di connessione a un nodo determinato dipende dal suo stesso grado di connettività. Questa specie di collegamento preferenziale in un sistema dinamico spiega quanto Watts e Strogatz non avevano notato, e cioè le leggi di potenza in una rete a invarianza di scala. Si tratta delle proprietà secondo cui l'informazione viene ad essere distribuita in un reticolo, indipendentemente dalla dimensione di quest'ultimo. Le reti a mondi piccoli che è dato riscontrare "là fuori", nel mondo reale, sono infatti contraddistinte da pochi nodi, detti "hub", con un altissimo numero di collegamenti, mentre la maggior parte dei nodi registra una bassa connettività. È la presenza di questi hub che offre la chiave per comprendere come mai le reti a mondi piccoli abbiano alti coefficienti di raggruppamento come le reti regolari e, però, come detto, con un ridotto grado di separazione media tra i nodi, come nelle reti casuali. Le "sottocomunità" che spontaneamente si determinano nella rete, sono densamente aggregate al loro interno, ma anche connesse tra di loro mediante i hub.

Per chiarire ulteriormente il punto, basterà mettere a confronto due reti con cui il lettore ha una certa dimestichezza; vale a dire, da un lato, il reticolo regolare del sistema di trasporto via terra illustrato, nel caso degli Stati Uniti, dalla figura 10:

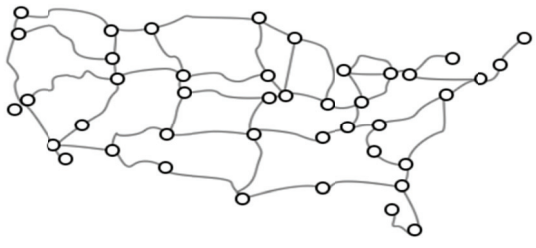

Figura 10: *Il reticolo regolare del sistema trasporti autostradale*

D'altro canto, si faccia caso a come cambia il reticolo nel caso del trasporto aereo:

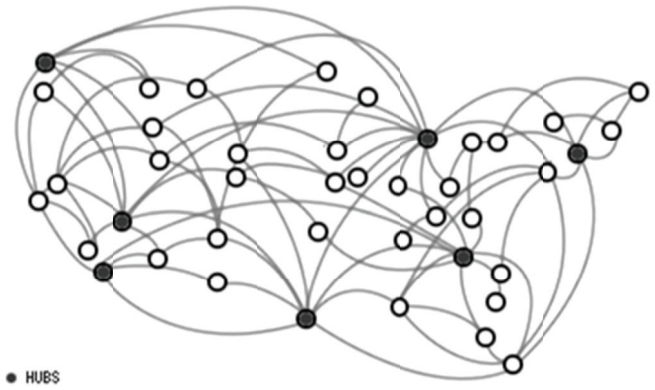


Figura 11: *Il reticolo a mondi piccoli del trasporto per via aerea*

Giunti a questo punto della nostra incursione nella teoria delle reti, immagino che il lettore abbia capito dove siamo andati a parare: nel corso degli ultimi anni abbiamo accumulato una mole di evidenza empirica che testimonia come il fenomeno dei mondi piccoli sia emerso spontaneamente su internet e nel web 2.0! Non è forse la complessità la scienza della sorpresa?

### 2.2.2.1. *I mondi piccoli di internet*

Da oltre dieci anni mi occupo della topologia d'internet e, cioè, dei modi in cui l'informazione fluisce attraverso i nodi di questa rete (Pagallo 2004 e 2005). Poco dopo le scoperte di Barabási sulle modalità a "mondi piccoli" d'internet e nel web dei primi anni duemila, mi avvicinai agli studi di Giancarlo Ruffo e al suo gruppo presso il dipartimento d'informatica a Torino, alle prese con i sistemi di condivisione file peer-to-peer (P2P) (Pagallo e Ruffo 2007; Pagallo e Ruffo 2012). Potete comprendere quale sia stata allora l'emozione di scoprire che, anche nel caso del sistema P2P Gnutella, la popolarità dei file audio e video nonché il comportamento degli utenti di quella rete si disponevano, ancora una volta, secondo le proprietà dei mondi piccoli! Presenza di hub o super-peer, alti coefficienti di raggruppamento, diametro accorciato e leggi di potenza…

Naturalmente, questo non significa che gli ordini spontanei di internet debbano per forza avere tali proprietà, così come, viceversa, che le proprietà delle leggi di potenza emergano soltanto nel mondo della rete. Anzi, dal punto di vista giuridico, è interessante rilevare come sia stato provato che anche il reticolo giurisprudenziale dei circa 26 mila pareri che la Corte suprema nordamericana ha pronunciato dall'inizio del 1800 al 2004, presentino tali proprietà (Chandler 2005); risultato che sarebbe stato in buona parte confermato dallo studio delle 30288 opinioni maggioritarie della stessa Corte tra il 1754 e il 2002 (Fowler e Jeon 2008). Ai medesimi risultati, poi, sarebbero giunti altri studi incentrati sui riferimenti interni al codice del-

l'ambiente francese (Boulet e al. 2010), alla Corte di giustizia UE (Malmgren 2011), e alla Corte suprema olandese (Winkels e de Ruyter 2012). In tutti questi casi, facendo salvi i diversi esponenti nella distribuzione della rete e la tara agli errori, si ha un reticolo in cui poche sentenze, pochi articoli, pochi file, ecc., fungono da ponte d'informazione per la gran massa dei nodi che compongono quel sistema. Riprendendo il grafico che la società italiana di statistica mette in mostra nel suo sito online, il risultato è una sorta di "lunga coda" illustrata dalla seguente figura:

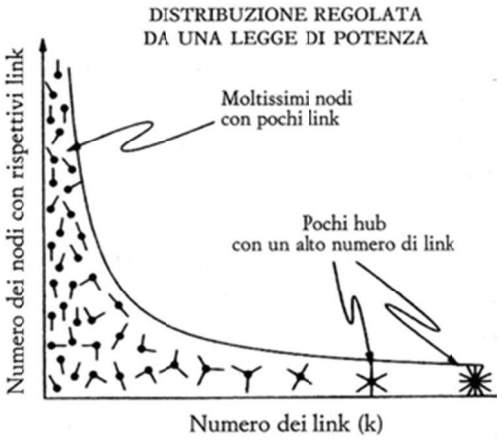


Figura 12: *La lunga coda*

A questo punto, sorge naturale la domanda: per quale motivo il comportamento collettivo che emerge più spesso da vaste reti di componenti individuali, senza alcuna forma di controllo centralizzato, né semplici regole d'istruzione, assume tuttavia questa fisionomia?

Probabilmente, la risposta va cercata nel fatto che questa sia la forma secondo cui, spontaneamente, si raggiunge l'equilibrio tra l'esigenza di far fronte alla complessità dei dati (e delle informazioni) con cui devono fare i conti gli agenti nella rete, e il modo per ottimizzare la distribuzione dell'informazione all'interno del reticolo in cui gli agenti si muovono. In forma altamente significativa, questa era stata del resto la tesi che sin dal 1969 aveva proposto il già ricordato Nobel per l'economia Herbert Simon, secondo cui la nozione di "gerarchia" era la chiave per cogliere l'architettura della complessità, oltre all'idea di "sistemi quasi scomponibili" che avrebbe dovuto conciliare gli approcci 'dal basso verso l'alto' con quelli verticistici. Con le parole di Simon, "i raggruppamenti ad alta intensità d'interazione nella mappa […] identificheranno una struttura gerarchica piuttosto ben definita" (Simon ed. 1996: 186). Più precisamente, secondo l'ipotesi del "mondo vuoto", l'idea di quasi-scomponibilità denota che "la maggior parte delle cose sarà soltanto debolmente connessa a quelle restanti; al fine di una descrizione accettabile della realtà soltanto una piccola frazione di tutte le interazioni possibili dovrà essere presa in considerazione" (*op. cit.*, 209). Tornando alla distinzione tra reticoli regolari, casuali e a mondi piccoli vista in precedenza, l'ipotesi di Simon sul "mondo vuoto" corri-

sponde così alla nozione di hub, nel senso che questi ultimi nodi non solo rappresentano i connettori comuni che accorciano le distanze tra i restanti nodi della rete, ma si accompagnano ai raggruppamenti ad alta intensità d'interazione presenti nella mappa delle relazioni sociali.

Tuttavia, non mancano, va da sé, problemi e questioni aperte: mi limito in questa sede a segnalarne tre. In primo luogo, che il comportamento sociale si auto-organizzi spontaneamente attraverso le modalità dei mondi piccoli, e/o mediante leggi di potenza, non garantisce affatto la costanza di tali comportamenti. Valga per tutti l'esempio, per certi versi, emblematico di Wikipedia, la nota enciclopedia in rete. Se il successo del sito è dipeso precisamente da un perno gerarchico sul quale hanno fatto leva i comportamenti spontanei di milioni di persone tra loro sconnesse, ciò nulla dice riguardo al (suo) futuro.

In secondo luogo, che una rete sociale si organizzi spontaneamente secondo le leggi dei mondi piccoli, allo stesso modo nulla dice sulla valutazione che dobbiamo dare di quella medesima rete. Basti dire che, una decina d'anni fa, il programma COPLINK è giunto alla conclusione che anche le reti dei narco-trafficanti si dispongono secondo le modalità dei mondi piccoli! Per essere più precisi, queste reti hanno "un diametro medio che varia da 4.5 a 8.5 gradi di separazione e possiedono una distribuzione a invarianza di scala con leggi di potenza aventi esponenti da 0.85 a 1.3" (Kaza et al. 2005).

In terzo luogo, dobbiamo fare i conti con l'impatto della rivoluzione tecnologica, senza la quale molti degli esempi di questo paragrafo non sarebbero stati immaginabili. Tanto i problemi che i mondi piccoli devono fronteggiare, quanto quelli che essi a volte creano, hanno più spesso una natura complessa, nel senso che investono, appunto, il complesso del sistema entro il quale si danno queste forme di ordine spontaneo. Si tratta di una nuova accezione del termine, dopo quelle di "complessità" in chiave algoritmica e quella esaminata fin qui sulla scia delle considerazioni di Hayek (e di Simon). A questa terza forma di complessità sarà dunque dedicata l'ultima parte del presente capitolo.

### 2.3. *I rischi del sistema*

Il terzo ed ultimo osservabile di questo capitolo richiama il concetto di "sistema", per segnalare come la complessità dei problemi con cui gli odierni ordinamenti giuridici sono chiamati a fare i conti, non riguardi soltanto la crescente mole di informazioni che tanto i legislatori, quanto i processi d'ordine spontaneo, sono tenuti a processare. In realtà, per via della rivoluzione tecnologica in corso, una delle principali novità che occorre prendere in considerazione, risiede nel fatto che i problemi di cui si tratta, formalizzabili in termini di "rischio", investono progressivamente la totalità del sistema, vale a dire che trascendono più spesso i tradizionali confini giuridici e politici degli stati nazionali sovrani.

Basti pensare con una metafora alla rete di internet come sistema nervoso degli attuali sistemi complessi, e ai diversi problemi che la rete pone ai livelli d'infrastruttura e riguardo allo strato logico e dei contenuti della rete. Le questioni che sorgono rispetto alla connettività e accesso al sistema, al dominio dei suoi indirizzi e alle innumerevoli controversie relative alla tutela dei diritti e alla prevenzione dei crimini,

difficilmente possono essere affrontate nel nome della sovranità dei singoli stati. Rispetto a un passato nemmeno tanto lontano, non solo i problemi delle società ICT-dipendenti attengono sistematicamente alla totalità del sistema in sé e per sé considerato, ma spesso sono significativamente affidati a organizzazioni transnazionali, più che internazionali o nazionali. Le competenze di ICANN, la quale è formalmente una società di diritto privato con sede in California, su cui avremo modo di insistere nei capitoli terzo e quarto, a proposito della gestione del dominio dei nomi in rete, risultano particolarmente indicative.

Per chiarire sin d'ora la novità dello scenario, è sufficiente soffermarsi sull'opera di un illustre sociologo, al quale si è già fatto cenno, Niklas Luhmann. Nonostante la versione del diritto che egli propone sollevi per molti versi gli stessi problemi in cui incorse, alla sua epoca, il "dio mortale" di Hobbes (v. sopra § 2.1.2.1), Luhmann, tra i cultori più noti della teoria dei sistemi, è stato soprattutto uno studioso attento alle dinamiche procedurali che hanno permesso ai sistemi giuridici di cambiar volto nel corso degli ultimi decenni. Ponendo l'accento sul livello d'astrazione che ha di mira l'informazione sulla realtà, la sociologia giuridica di Luhmann propone, da questo punto di vista, due variabili alla nostra indagine, come illustra l'ultima figura del presente capitolo:

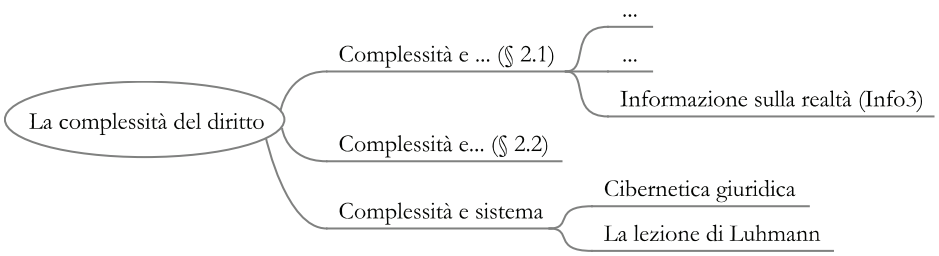


Figura 13: *La teoria dei sistemi*

A continuazione (§ 2.3.1), torneremo su alcune nozioni chiave di questo volume, come complessità, informazione e diritto; ma, appunto, secondo la prospettiva sociologica elaborata da Luhmann tramite la teoria dei sistemi e la sua versione cibernetica del diritto.

Dopo di che (§ 2.3.2), la lezione di Luhmann consisterà nello spiegare perché le sfide poste dalla rivoluzione tecnologica, "i rischi del sistema", vadano oggi affrontati sul piano della governance, e non solo su quello tradizionale del governo.

### 2.3.1. *Cibernetica giuridica*

L'intento di Luhmann è stato di rappresentare il diritto come sistema autopoietico e auto-referenziale, capace cioè di determinare dal proprio interno il confine o chiusura rispetto all'esterno, tra input e output, tra sistema, appunto, e ambiente. Nello stesso modo in cui un organismo biologico, per sopravvivere come ente a sé stante, deve generare una chiusura operativa che è inseparabile dal suo stesso essere autonomo, così il diritto deve essere in grado di raggiungere un equilibro tra

ciò che è dentro e ciò che è fuori, tra la capacità vitale di dotarsi di un'auto-organizzazione e rispondere, al tempo stesso, alle sollecitazioni, impulsi o sfide dell'ambiente. Nel caso degli organismi biologici, il fine è la sopravvivenza allo scopo di riprodursi attraverso la progenie: nel caso del diritto, trattandosi di un ente artificiale, il fine va da sé è un altro. Oltre al formalismo istituzionale, si tratta di porre un limite all'indeterminata serie di scelte, più o meno etiche, dei consociati, tramite una serie di procedure non arbitrarie tese a filtrare la complessità di tali scelte. Con le parole (spesso ostiche) dei *Sistemi sociali*, "complessità vuol dire necessità di selezione, necessità di selezione significa contingenza, contingenza significa rischio" (Luhmann ed. 1990: 95).

Con parole più semplici, scopo del diritto è quello di riconfigurare le aspettative del comportamento sociale, in modo da far chiedere, invece del perché, il come. Alla luce del paragone con gli organismi biologici, il diritto funge, cioè, da sistema immunitario per l'intero tessuto sociale, nel senso che mira a sgravare gli individui dalla fatica di chiedere ogni volta, in prima persona, il perché della decisione giuridica riguardo, ad esempio, al pagare le tasse, alle regole del codice della strada, e via discorrendo.

La selezione delle regole giuridiche, volte a ridurre la complessità che deriva dalla pressione ambientale del sistema, deve naturalmente prendere in considerazione come gli individui reagiscano a tale selezione: è l'aspetto della "retroazione" o *feedback* che Luhmann riprende dagli studi di cibernetica, ai quali si richiama espressamente. "Secondo le assunzioni generali della teoria dei sistemi, dalle quali prendiamo qui le mosse, sussiste tra autoregolazione e riferimento all'ambiente una connessione tale che un sistema può adattare se stesso agli avvenimenti rilevanti del suo ambiente come pure può mutare il proprio ambiente tenendo conto di aspetti rilevanti per il sistema stesso" (Luhmann ed. 1978: 120). Tuttavia, anche se ci limita agli avvenimenti rilevanti dell'ambiente, il punto di vista adottato da Luhmann è quello interno al sistema prescelto: la necessità di tener conto del feedback dei consociati non ha alcuna suggestione morale, etica o democratica nel campo del diritto. Piuttosto, l'effetto di retroazione della cibernetica giuridica è un indicatore di tipo operativo, che serve al sistema per mantenere il suo equilibrio ed efficienza funzionale. Del resto, c'è del vero in quel che dice Luhmann quando osserva che, entrando in un tribunale, in un ospedale, in un ufficio postale, o in un'aula universitaria, spesso l'individuo ha l'impressione di essere un mero ingranaggio della macchina giuridica, quasi fosse, cioè, semplice rumore o ambiente di se stesso.

Nondimeno, esistono tutta una serie di ragioni, sia tecniche, sia filosofiche, sia sociologiche, che mettono in dubbio il tentativo di Luhmann di concepire il diritto come una macchina cibernetica auto-referenziale, vale a dire in grado di stabilire dal proprio interno ciò che è incluso o, al contrario, viene espunto dal sistema. Anche ad ammettere, senza concedere, che il diritto sia soltanto, al modo di Luhmann, una questione di potere e di agire strategico, basterebbe solo ricordare ciò che viene insegnato agli studenti di giurisprudenza del primo anno, a proposito di quella particolare classe di fonti fatto chiamata fonti *extra* e *contra ordinem*. A ribadire il fenomeno dell'incompletezza ricordato in precedenza (§ 2.1.3), è sufficiente riportare le parole di Livio Paladin (1933-2000), già presidente della Corte costituzionale italiana, per cui "nessun elenco e nessun sistema degli atti e dei fatti normativi, quand'anche fis-

sati dalla stessa Costituzione di un determinato ordinamento statale positivo, potranno mai essere assolutamente tassativi e compiuti: vale a dire sottratti a ogni divenire delle fonti, indipendentemente dalle formali revisioni di quella disciplina costituzionale" (Paladin 1996: 18-19).

Ma, come riferito, non è certo questo aspetto caduco della cibernetica giuridica di Luhmann sul quale vale la pena d'insistere. Piuttosto, occorre soffermarsi sul modo in cui egli ha saputo cogliere i meccanismi che consentono ai sistemi giuridici di evolvere e "tali da mettere in relazione tra loro un ambiente variabile e un sistema variabile" (Luhmann 1978: 120). Sulla base della sua lezione, avremo modo di capire come siano venute mutando, nel frattempo, le fonti del diritto, nel passaggio dalle tradizionali forme di governo a quelle odierne della governance.

### 2.3.2. *La lezione di Luhmann*

La nozione di rischio alla quale si è fatto cenno sulla scorta di alcune tesi di Luhmann, non è naturalmente l'unica: a ben vedere, il problema è tanto antico quanto la stessa evoluzione umana. Per dirla con l'introduzione di *Analisi del rischio e società*, "quando i gruppi delle famiglie nel Neolitico condivisero conoscenza e risorse per combattere la fame, la sete, il clima, o attacchi dall'esterno, essi stavano tentando di venire a capo del rischio che avevano di fronte […] La gestione del rischio ha rappresentato una motivazione fondamentale per lo sviluppo delle strutture sociali e di governance negli ultimi 10 mila anni" (McDaniels e Small 2004).

Naturalmente da allora, come suol dirsi, molta acqua è passata sotto i ponti: da un lato, negli ultimi cento anni, si è affermato un fiorente settore di studi, nel campo della gestione del rischio, volto a definire una metodologia che sia capace di affrontare fattori che possono essere di difficile o perfino impossibile quantificazione. D'altro canto, come riferito all'inizio di questo paragrafo, tale rischio è diventato sistemico, nel senso che investe la società nel suo complesso. Come afferma un altro sociologo tedesco, Ulrich Beck (n. 1944), nel suo fortunato volume *Risiko Gesellschaft* o *La società del rischio* (1986), "la tesi è che, mentre nella società industriale classica la logica della produzione della ricchezza prevaleva sulla logica della produzione del rischio, nella società del rischio questa relazione è stata capovolta" (Beck ed. 2000).

Per comprendere come gli ordinamenti giuridici si siano riposizionati di fronte a questo capovolgimento, tornano dunque utili le indicazioni metodologiche di Luhmann, proprio perché il rischio, a suo avviso, è connaturato alla pretesa auto-organizzativa del diritto a tre distinti livelli:

i) il rischio innanzitutto si profila sul fronte dell'input, vale a dire come fattore d'incertezza al quale il sistema giuridico deve far fronte;

ii) il rischio riappare sul fronte dell'output, come conseguenza del bisogno che il diritto ha di scegliere tra risposte diverse, esponendosi così alla contingenza;

iii) dalla "doppia contingenza" che dipende sia dalle richieste sociali (input), sia dalla pretesa di armonia interna al sistema in vista della sua resa (output), segue l'incertezza relativa al coordinamento tra i due livelli.

Per dirla ora con Luhmann, "nella prassi decisionale interna (prassi selettiva) al posto della determinazione di relazioni non contingenti tra elementi contingenti su-

bentrano degli indicatori di tipo operativo. Il sistema, per così dire, osserva se stesso se qualcosa nella propria relazione con l'ambiente stia mutando, sia problematica, debba essere corretta. In sistemi che possono differenziare al loro interno i problemi dell'input dai problemi dell'output, tali indicatori servono, nel contempo, come regole della coordinazione tra input e output. Essi controllano il passaggio dall'input all'output" (Luhmann 1978: 121).

Tradizionalmente, nei primi secoli dell'era moderna, questo passaggio dal primo al secondo livello di rischio, è stato affidato agli organi di governo su scala nazionale. L'aumento di complessità ingenerato dal primo livello, tuttavia, non solo ha revocato in dubbio l'adeguatezza della risposta normativa sul fronte dell'output; ma, nel gergo di Luhmann, i problemi dell'output hanno indotto un riposizionamento sul terzo livello, su come cioè il sistema giuridico debba essere internamente differenziato al fine di correggere la propria relazione con un ambiente radicalmente mutato, perché oltremodo complesso. Questo riposizionamento lo si registra sia sul piano istituzionale, sia sul piano delle fonti. Mentre quest'ultimo tema sarà l'oggetto del capitolo quarto, conviene per intanto proseguire la nostra analisi, esaminando il passaggio che ha condotto dai tradizionali organi di governo a quelli dell'odierna governance. Come diremo a continuazione, questo passaggio getta ulteriore luce sulle tre accezioni di complessità analizzate nel presente capitolo. Secondo la lezione di Luhmann, il sistema giuridico ha infatti dovuto riposizionarsi in questo modo sul fronte della "doppia contingenza", innanzi alle sfide della complessità.

# III.
# *Governance*

> "Mentre avanzavo lentamente verso di lui, notai che era pallido, con l'aria stanca e una lunga barba grigia; aveva in capo un berretto azzurro con un gallone d'oro stinto, indossava una giacca rossa e un paio di calzoni *tweed* grigio … 'Il dottor Livingstone, suppongo!' 'Sì', egli rispose con un sorriso gentile, alzando leggermente il berretto"
>
> Henry MORTON STANLEY

Il presente capitolo sulla "governance" si occupa della dinamica dei processi istituzionali in corso, per contrapposizione alla statica del sistema, rappresentata dalle fonti del diritto, di cui si dirà nel capitolo che segue. Come premessa del discorso, occorre notare un fatto curioso, ma essenziale. A differenza di altri lemmi inglesi invalsi nell'italiano scritto e parlato, dove pure avrebbero una loro traduzione esatta – come nei casi già menzionati di *feedback* o retroazione, *computer* o calcolatore elettronico, *privacy* o riservatezza, e via discorrendo – non esiste traduzione italiana per il termine di *governance* (salvo ricorrere al termine, raro e desueto, di governamento o, ricorrendo ai neologismi, parlare di una nuova "governanza").

La circostanza non è priva di conseguenza poiché, spesso, il termine inglese serve a denunciare oscuri meccanismi istituzionali anti-democratici, tecnocratici, o la semplice mancata trasparenza di governo (Vitale 2008). Alcuni si peritano di spiegare che si tratta di "una parola senza senso. O per meglio dire: un concetto il cui senso risiede proprio nel non averne uno" (Andronico 2012). Altri, a proprie spese, semplicemente lo ignorano: è sufficiente dare una scorsa ai volumi e manuali universitari sulle forme di stato e di governo, per rendersene conto (es. Pinelli 2009).

Del resto, in queste denunce, incomprensioni o ignoranza di fondo che distingue la letteratura italiana sul tema – in contrasto con il dibattito occorso presso le Nazioni Unite negli ultimi quindici anni – c'è un grano di verità. Ricapitolando i problemi emersi nei precedenti capitoli di questo libro, abbiamo visto che la rivoluzione tecnologica ha prodotto, innestato, oppure accelerato, profonde trasformazioni sociali che hanno reso oltremodo complessi gli odierni dilemmi degli ordinamenti giuridici, per tre ragioni tra di loro connesse.

Innanzitutto, il rimando va alla complessità relativa all'aumento dell'informazione necessaria per affrontare o capire i fenomeni in corso, che nondimeno si accompagna alla difficoltà di comprimere algoritmicamente detta informazione. Un esempio lampante è offerto da quella forma di governance su scala europea che è l'Unio-

ne: a cinquant'anni di distanza dalla famosa sentenza della Corte di giustizia di Lussemburgo nel caso *van Gend & Loos* (1963), vale ancora la tesi della Corte che quello dell'Unione è "un ordinamento giuridico di nuovo genere nel campo del diritto internazionale".

In secondo luogo, dalla complessità dei fenomeni in corso sono spontaneamente emerse forme d'ordine sociale, che a fatica possono trovare sistemazione con le categorie tradizionali dei giuristi. Come detto in § 1.4.3, capita spesso che gli individui preferiscano seguire nella rete di internet consuetudini e usi che, con tutta evidenza, non è dato ricondurre né al diritto nazionale né al diritto internazionale. L'opportunità di scelta tra ordinamenti diversi che era appannaggio esclusivo delle imprese multinazionali, è stata per così dire democratizzata, in controtendenza alle denunce sul potere anti-democratico o tecnocratico degli ordinamenti posti in essere da quelle stesse multinazionali.

Infine, i fenomeni con cui sono alle prese gli ordinamenti giuridici odierni sono vieppiù complessi perché investono tali ordinamenti nel loro insieme, obbligandoli a riposizionarsi. Per rimanere agli esempi già fatti, basti riflettere ancora sul processo d'integrazione europea e al modo, beninteso complesso, in cui s'intrecciano le sue norme con quelle degli stati membri. La necessità di inquadrare i tradizionali poteri di governo in un più ampio reticolo istituzionale – spesso compendiato, appunto, con la parola "governance" – non fa che riportare alla confusione concettuale di molti studiosi italiani, dalla quale abbiamo preso le mosse in questo capitolo.

Per capire di cosa si tratti e quale sia la posta in gioco, nel passaggio dalla vecchia nozione di governo a quella odierna della governance, conviene partire dalla radice latina che accomuna i due termini, ossia il "gubernum" come timone della nave. Per traslato, la parola non soltanto ha indicato l'arte del condurre una nave, e cioè di governarla; ma, fatto ancor più interessante, questa nozione di governo, declinata come "gubernaculum", si è indissolubilmente intrecciata sin dal medioevo con il termine "iurisdictio", al punto che la coppia concettuale divenne un "luogo comune della teoria politica europea del tardo '200" (McIlwain 1990: 98).

Nonostante la derivazione del nostro odierno termine "giurisdizione" dall'antica iurisdictio, dobbiamo però resistere alla tentazione d'intendere il passato con le lenti del presente, onde comprendere meglio l'odierno passaggio dal governo alla governance in rapporto all'evoluzione dei termini in questione. Tanto il gubernaculum, quanto la iurisdictio, infatti, vanno colti all'interno di ciò che oggi chiameremmo governo per opposizione ai poteri giurisdizionali dei giudici. La differenza consiste nel fatto che, mentre nell'ambito del gubernaculum, i poteri del sovrano medioevale erano assoluti, tali poteri erano invece limitati nell'ambito della iurisdictio. Questa fondamentale distinzione, messa a punto dal grande Henry de Bracton (ca. 1210-1268), in *Delle leggi e consuetudini inglesi*, sarebbe stata ripresa da John Fortescue (ca. 1394-1480), opponendo il potere regale a quello politico del re; e, infine, dal padre putativo del common law moderno, Edward Coke (1552-1634). Nella sua opposizione alle pretese assolutistiche di re Giacomo I (1566-1625), Coke riconosceva le prerogative del sovrano per alcune attività come l'imporre le tasse, il batter moneta e, come diremmo noi oggi, per gestire la politica estera; ma, nell'ambito della iurisdictio, vale a dire riguardo alla vita e alla proprietà dei sudditi, i poteri del sovrano erano limitati dalla legge. "Del che – come ricorda personalmente Coke nei

*Report*, riportando il famoso discorso da lui tenuto il 10 novembre 1607 davanti a Giacomo in persona e a tutte le maggiori autorità del regno – il Re si sentì gravemente offeso, e disse che allora egli era sottoposto alla legge, e che era tradimento affermare una tale cosa, come egli disse; al che io [Coke] dissi che Bracton affermava che il Re non deve essere sottoposto agli uomini, bensì a Dio e alla legge" (in Matteucci 1962: 56).

Due erano i maggiori limiti dell'antica iurisdictio, che avrebbero poi condotto all'odierna concezione del termine giurisdizione. Il primo limite concerneva la mancanza di un'effettiva sanzione nel caso della violazione da parte del re, dei limiti fissati dalla legge. Il secondo difetto dipendeva dall'incerto confine tra le due sfere che, non a caso, con la morte di Giacomo e la successione al trono di suo figlio Carlo (1600-1649), avrebbe finalmente condotto allo scoppio della guerra civile in Inghilterra. Da un lato, il Re e i realisti a difesa dei poteri assoluti regi, delle sue prerogative; di contro, il Parlamento e i giudici della corona a difesa della iurisdictio con i diritti dei sudditi. Per dirla ancora con Charles McIlwain, "una parte rivendicava la lettera e l'altra lo spirito delle istituzioni monarchiche inglesi" (McIlwain 1990: 151).

Da ben due guerre civili e con la "gloriosa Rivoluzione" del 1689, l'Inghilterra ne sarebbe uscita con un assetto costituzionale nuovo, in cui cominciano a plasmarsi le categorie alle quali siamo tuttora abituati: si tratta infatti di una nuova responsabilità per gli atti del governo che non riguarda più soltanto la sfera della iurisdictio, ma l'intero spettro del gubernaculum. Per riprendere la terminologia dei manuali universitari oggi in voga, si può dire in altri termini che, nel mutare la forma del gubernaculum, muta anche la forma di stato: dalla monarchia assoluta preconizzata da Giacomo, che sarebbe poi costata la testa a suo figlio Carlo, si passa alla monarchia costituzionale liberale d'inizio Settecento.

La morale da trarsi da questi brevi, ma doverosi cenni storici, è chiara: per comprendere ciò che muta con l'odierno passaggio dalla nozione tradizionale di governo, che comincia a forgiarsi nel Regno Unito tra Seicento e Settecento, all'attuale figura della governance, bisogna prestare attenzione a come è venuta evolvendo la dialettica del diritto tra gubernaculum e iurisdictio. Su queste basi, sarà poi dato valutare quel reticolo istituzionale compendiato al giorno d'oggi, appunto, con l'idea di governance. La prima figura di questo capitolo s'incarica d'illustrare il punto con i suoi quattro osservabili:

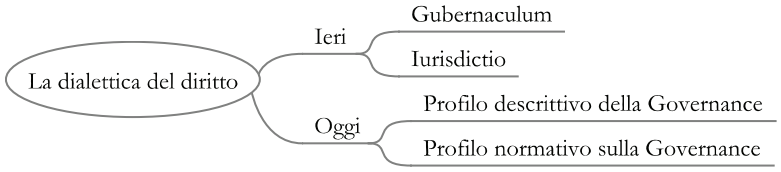


Figura 14: *Archeologia e forme della governance*

A continuazione (§ 3.1), esamineremo come l'idea di gubernaculum sia venuta evolvendo dopo gli eventi rivoluzionari inglesi, allo scopo di comprendere cosa cambi con l'attuale governance. Tre varianti di questa evoluzione sono di particolare inte-

resse: la variante liberale (§ 3.1.1), quella democratica (§ 3.1.2), e quella costituzionale (§ 3.1.3).

Dopo di che (§ 3.2), proprio a partire della variante costituzionale di governo, prenderemo in considerazione come l'idea di iurisdictio sia a sua volta venuta mutando con i poteri delle corti costituzionali (§ 3.2.1), e nel quadro dell'integrazione europea (§ 3.2.2). Su queste basi, passeremo a esaminare le odierne dinamiche istituzionali della governance (§ 3.3), prendendo spunto dal già menzionato dibattito occorso presso le Nazioni Unite quasi due decenni fa. Più in particolar modo, si tratterà di distinguere tra settori (§ 3.3.1), e livelli della governance (§ 3.3.2), per concentrarci sui suoi modelli globali e, avendo a mente l'oggetto del presente libro, sull'impatto della tecnologia sugli odierni sistemi giuridici, soprattutto sulla governance globale d'internet.

Nella parte conclusiva del capitolo (§ 3.4), l'indagine sulla governance d'internet sarà ulteriormente approfondita, al fine di tirare le fila del discorso fin qui svolto a proposito di tecnologia, complessità e governance. Alla luce del modo in cui, tanto gli organi del gubernaculum, quanto quelli della iurisdictio, si sono occupati della rete (§ 3.4.1), sarà reso evidente il passaggio dal tradizionale piano del governo a quello attuale della governance, dando conto del complesso reticolo istituzionale che comprende sia attori privati sia organismi pubblici (§ 3.4.2). L'indagine si soffermerà infine sui problemi e le questioni che si sono aperte al giorno d'oggi (§ 3.4.3), proponendosi al riguardo tre criteri grazie ai quali prendere posizione in termini di onere della prova, dovere di conoscenza e scelta degli strumenti normativi. In questo modo, saremo pronti a passare dalla dinamica allo studio della statica del sistema: le fonti del diritto (capitolo quarto).

## 3.1. *Le avventure del gubernaculum*

È opinione condivisa che gli ordinamenti giuridici d'Occidente, oggi, possano riassumersi con la formula dello stato costituzionale di diritto, o stati liberal-democratici. Se mai, le differenze ruotano tra forme accentrate, regionali o federali di stato, tra forme presidenziali o parlamentari di governo, e via dicendo. Per capire come le forme del gubernaculum siano venute evolvendo nel corso degli ultimi tre secoli, a partire dall'istituzione della monarchia costituzionale britannica, pare dunque opportuno concentrarsi sulle tre principali variabili del primo osservabile di cui alla figura 14, ossia il liberalismo di John Locke (1632-1704), il contrattualismo democratico di Jean-Jacques Rousseau (1712-1778), e le tesi dei padri fondatori della Repubblica statunitense, tra cui, per le ragioni che diremo, un particolare cenno va sin d'ora a Thomas Jefferson (1743-1826). Iniziamo, di qui, la nostra disamina sulle avventure del gubernaculum, con l'opera di chi è spesso considerato il padre del liberalismo moderno e delle dichiarazioni dei diritti dell'uomo, vale a dire Locke.

### 3.1.1. *Il giusnaturalismo di Locke*

In contrapposizione alla variante assolutistica del contratto sociale di Hobbes, di cui si è già detto (§ 2.1.2.1), Locke ne offre la classica versione liberale nei *Due trattati sul governo* pubblicati anonimi proprio nell'anno della rivoluzione inglese (1689).

La distinzione tra queste due versioni del contrattualismo riguarda basicamente come intendere la premessa stessa del discorso, vale a dire lo stato di natura. Come si è già visto, per Hobbes, lo stato di natura rappresenta quella condizione bellica esemplificata dalle guerre civili che, del resto, lo stesso Hobbes ebbe modo di vivere personalmente ai tempi del regno di Carlo I. Per Locke, invece, esistono veri e propri diritti che appartengono allo stato di natura che, poi, corrispondono a quelli rivendicati per secoli dai sudditi inglesi contro le pretese assolutistiche dei loro monarchi. Questi diritti corrispondono alla vita, alla libertà e agli averi, che Locke riassume spesso con una parola sola: "proprietà". Per questo verso, Locke sembra dunque rifarsi sia alla tradizione classica del giusnaturalismo, sia all'eredità del common law in tema di iurisdictio. Tuttavia, ci sono due differenze fondamentali.

Da un lato, rispetto al common law, Locke è un filosofo, non un giurista; egli non si accontenta di fondare i diritti dello stato di natura per via consuetudinaria e, cioè, come aveva fatto ancora Edward Coke, adducendo che quei diritti vanno riconosciuti come tali perché, in realtà, essi esistono "da sempre", da tempo immemorabile. D'altro canto, nel fondare su basi razionali, e non storiche, tali diritti, Locke si allontana dalle scuole classiche del diritto naturale, perché mira a giustificare tali diritti sulla base di concetti morali creati artificialmente dall'uomo e facendo leva sulla motivazione egoistica che orienta l'agire degli individui. Questa impostazione ha fatto sí che, in Locke, a mala pena convivano i principi epistemologici e giusnaturalistici della sua dottrina, tra utilitarismo e leggi naturali di Dio, che tanto cruccio hanno provocato tra gli studiosi e interpreti del suo pensiero. Infatti, rimane altamente problematico come "conciliare la sua visione di una società dinamica costituita da individui egoisti, con la dottrina giusnaturalistica classica della convivenza secondo virtù e giustizia degli uomini dello Stato […] Come è possibile che i concetti creati artificialmente dall'uomo colgano la legge di natura non emanata dall'uomo e senza dubbio trascendente la coscienza umana stessa?" (Euchner 1976: 244 e 177).

Ma, anche a lasciar perdere la coerenza filosofica degli assunti di fondo, tra le leggi naturali di Dio e i diritti naturali dell'uomo, occorre porre un'ulteriore domanda: se gli uomini godono di diritti allo stato di natura, perché mai, proprio come Hobbes, è necessario abbandonare tale stato?

La ragione, per Locke, dipende dal fatto che, pur godendo di tali diritti, possono sorgere controversie tra gli uomini circa il "mio" e il "tuo", per cui il potenziale conflitto che ne discende può essere superato soltanto a una condizione, e cioè che gli individui rinuncino al proprio diritto naturale di farsi giustizia da sé. Mentre, nel caso di Hobbes, il contratto sociale appare come un atto di rinuncia unilaterale in favore del terzo sovrano, nel caso di Locke il contratto sociale consiste in un sinallagma, o contratto a prestazioni corrispettive. Gli individui rinunciano al loro diritto di farsi giustizia da sé nel dirimere le proprie controversie, a condizione che tutti i restanti diritti naturali, compendiati nella proprietà, siano garantiti nella istituenda società civile. Ecco perché, a differenza di Hobbes, Locke evita di utilizzare il termine di sovrano, impiegando piuttosto quello di arbitro o di supremazia, per denotare il carattere dell'autorità politica; come quando, ad esempio nel § 87 del secondo trattato, afferma, a proposito dell'istaurazione della società civile, che "la comunità diviene arbitra"; o, nel § 157, allorché presenta la costituzione del governo civile, o potere legislativo, come la "suprema deliberazione" della società.

Per questo verso, Locke appare dunque precursore delle dichiarazioni dei diritti dell'uomo e padre del liberalismo moderno, in quanto i diritti degli individui preesistono alla istituzione della società civile e, anzi, i poteri di prerogativa del vecchio gubernaculum sono limitati dal rispetto e garanzia verso tali diritti. Ma, che dire nel caso dell'abuso di potere, nel caso in cui, cioè, governati e governanti entrino in conflitto?

Manca infatti in Locke ciò che oggi chiameremmo organo di chiusura del sistema, dato che il fondamento della prerogativa del governo è, a suo avviso, "il medesimo potere esecutivo della legge di natura posseduto dagli individui e sul quale si basa in ultima istanza la forza obbligante della stessa legge positiva" (Dunn 1992: 174). In questo gioco di specchi, Locke non si propone di definire ciò che per sua natura appare come indeterminato, vale a dire, con le parole del filosofo, il potere della prerogativa del governo intesa come "il potere di fare il pubblico bene senza una norma". Piuttosto, l'idea è di determinare questi poteri in negativo, fissandone i limiti attraverso una lista di ciò che non si può fare. Alla base del nesso tra governati e governanti, emerge in questo modo una contraddizione di fondo che prende le vesti di un doppio fondamento: il carattere fiduciario della relazione politica si basa sul contratto sociale che, a sua volta, rinvia a un ordine di verità che dovrebbe essere intellegibile per tutti. Mancando, però, un organo della iurisdictio e la procedura con cui far fronte al caso di conflitto tra governati e governanti, si finisce in una diabolica alternativa:

– o l'accento cade sulla fiducia che deve legare chi governa ai governati, per cui diventa legittima qualsiasi distribuzione di potere che gli uomini accettino come tale; ma, allora, non si vede quale sia il ruolo dei diritti inalienabili dello stato di natura;

– oppure, sorge un nuovo diritto, quello di resistenza, come diritto individuale d'iniziativa per fare appello onde restaurare il grado preesistente di legalità. Questa via, che è poi quella seguita da Locke, riporta nondimeno al punto di partenza della riflessione di Hobbes sullo stato di natura. Per venire a capo del problema, la variante liberale del contratto sociale si riallaccia di qui al pensiero politico medioevale, secondo la conclusione che si ha nel § 241 del secondo trattato di Locke: in breve, sarà soltanto Dio a decidere, in ultima istanza, a quale delle due parti spetti la ragione, concedendone la vittoria sul campo di battaglia.

Gli interpreti di Locke hanno fornito varie ragioni per spiegare questo apparente paradosso che riporta le conclusioni del padre del liberalismo moderno agli appelli alla divinità tipici della cultura medioevale. Si tratterebbe della centralità del motivo religioso lungo tutta la riflessione di Locke e del fatto che non si sia preoccupato, a differenza di Hobbes, di alcun vuoto etico, dato che Locke avrebbe dato piuttosto voce alla speranza e concordia della gloriosa Rivoluzione.

Ma, ai fini della presente indagine, è sufficiente menzionare un elemento cruciale: avrebbe dovuto trascorrere un intero secolo, dopo i *Due trattati sul governo*, per avere una più soddisfacente teorizzazione dei poteri della iurisdictio.

### 3.1.2. *La democrazia di Rousseau*

Dopo i brevi cenni sul padre fondatore del liberalismo, seguono quelli sul padre indiscusso della democrazia moderna: Jean-Jacques Rousseau. Personaggio complesso e, per molti versi, enigmatico, gli studiosi si dividono ancor oggi su come interpreta-

re la sua opera. A distanza di tanti anni dal *Contratto sociale* (1762), desta ancor oggi stupore come un così piccolo libro abbia inciso sulla cultura occidentale, elevando a modello ciò che invece, per secoli, era apparsa l'eccezione e, nel migliore dei casi, la forma di stato (e di governo) adatta solo alle repubbliche di ridotte dimensioni: la democrazia.

Ancora una volta, come già per Hobbes o Locke, l'intento non è di dar conto in maniera esaustiva di tutti gli aspetti della riflessione di Rousseau: piuttosto, si tratta di metterne in luce quei profili che appaiono tuttora rilevanti per il modello liberaldemocratico delle istituzioni odierne. Il punto di partenza è dato dalla nozione di libertà intesa, come già in Hobbes, come capacità di fare tutto ciò che si vuole. Siccome tutti gli uomini ambiscono a tale identità tra volere e potere, come si può dunque essere liberi, vivendo insieme agli altri? Come evitare il caos? Oppure, per dirla con Rousseau, come "quadrare il cerchio della politica"?

Riprendendo la struttura argomentativa della tradizione, anche Rousseau muove, per risolvere il problema, dalla nozione dello stato di natura. Rispetto ai predecessori, tuttavia, ci sono due sostanziali innovazioni. Da un lato, Rousseau dichiara apertamente che lo stato di natura è una mera ipotesi di lavoro, e non una condizione reale in cui mai si sia trovato l'uomo: occorre nondimeno procedere da questa convenzione se s'intende gettar luce sulla condizione in cui gli uomini versano nel mondo reale, vale a dire il fatto che gli uomini non siano liberi, non potendo per lo più fare ciò che vogliono.

D'altro canto, l'uomo dello stato di natura non è né l'uomo in potenziale guerra di Hobbes, né l'uomo proprietario di Locke, bensì un soggetto unico che, proprio perché tale, è assunto come libero, cioè, come dice Rousseau nell'ottavo capitolo del *Contratto sociale* (ed. 1997: 29), "non ha per limiti che le [sue] sole forze". Muovendo pertanto da quest'ipotesi dell'uomo libero allo stato di natura, la nuova finalità che il contratto sociale assume nella versione democratica di Rousseau è di mantenere questo stato nel passaggio dalla libertà dell'essere unico nello stato di natura, alla libertà che si dà nel convivere con gli altri nella società civile. Come ciò sia possibile è presto detto: tramite il contratto sociale che ciascuno di noi fa con se stesso. Con le parole del filosofo, "ciò che l'uomo perde col contratto sociale è la sua libertà naturale e il diritto illimitato su tutto quello che lo tenta e che può essere da lui raggiunto; ciò che egli guadagna, è la libertà civile e la proprietà di tutto quello che possiede" (*ibidem*).

Ma, anche in questo modo, concluso il contratto di ciascuno con se stesso, torna la domanda formulata in precedenza: in che senso potremo rimanere liberi nella società civile?

Senza entrare nel merito delle differenze, anche fondamentali, che separano la forma di democrazia diretta preconizzata da Rousseau, dalle odierne democrazie di tipo rappresentativo, la risposta passa attraverso il meccanismo procedurale che conduce alla nozione chiave di "volontà generale". In sostanza, quando giunge il momento delle decisioni da prendere nella società civile, ogni individuo, divenuto cittadino, è chiamato a dare il suo voto in seno all'Assemblea. La legge, che è il risultato di quel voto, non limita pertanto la libertà dei cittadini perché, votandola, essi hanno voluto quella legge e, quindi, quest'ultima non limita ma anzi coincide con il nuovo potere che i cittadini hanno acquisito a séguito del contratto sociale.

Senonché, come detto, le cose non sono mai semplici con Rousseau: la nozione

di volontà generale che egli propone come fondamento della legge, può infatti intendersi in due modi affatto diversi. Per un verso, si legge nel *Contratto sociale*, "quando si propone una legge nell'assemblea del popolo, ciò che si domanda ai cittadini non è precisamente se essi approvino la proposta oppure la respingano, ma se essa è conforme o no alla volontà generale, che è la loro: ciascuno dando il suo voto esprime il suo parere; e dal calcolo dei voti si trae la dichiarazione della volontà generale" (*op. cit.*, p. 144). Alla luce di questa prima definizione, si può dunque dire che la volontà generale sia il prodotto della somma algebrica dei voti espressi in assemblea, ossia quanto il 50 più 1% del voto stabilisce. Ma, come la mettiamo con chi non partecipa della maggioranza assembleare, e cioè con chi, votando, rimane in minoranza? In che senso continuerebbe a essere libero?

La risposta di Rousseau è sorprendente: "quando dunque prevale il parere contrario al mio, ciò non significa altro che mi sono ingannato, e che ciò che credevo essere la volontà generale non era tale" (*op. cit.*, p. 144). Avendo presente le drammatiche esperienze dei regimi totalitari del secolo scorso che, tra l'altro, hanno visto Hitler giungere democraticamente al potere, non è un caso se numerosi studiosi sono venuti scorgendo, nel pensiero di Rousseau, non tanto il padre fondatore della democrazia moderna ma, piuttosto, il precursore del totalitarismo del Novecento (Talmon ed. 2000).

D'altro canto, in un altro passo del *Contratto sociale*, è sempre Rousseau a offrire una definizione alternativa del concetto di volontà generale, allorché non solo ammette che la maggioranza in assemblea possa sbagliare ma, addirittura, che ciò possa accadere perfino alla volontà di tutti. Con le sue parole, "vi è spesso molta differenza tra la volontà di tutti e la volontà generale; questa mira soltanto all'interesse comune; l'altra all'interesse privato e non è che una somma di volontà particolari: ma togliete da queste volontà il più e il meno che si distruggono a vicenda, resta quale somma delle differenze la volontà generale" (*op. cit.*, p. 42). Anche in questo caso, però, non mancano i problemi: ne segnalo tre.

In primo luogo, se la volontà generale appare la condizione affinché l'assemblea voti politicamente in vista dell'interesse comune, più che il risultato del voto espresso in assemblea, come sembra del resto suggerire Rousseau attraverso la funzione educatrice della figura mitica del Legislatore, perché mai dare il voto all'assemblea?

In secondo luogo, a conferma di questo dubbio, valga riassumere i tre snodi del discorso in termini matematici:

i) V = P. Questa condizione d'identità tra volere e potere, nei limiti "delle sole forze dell'individuo", rappresenta l'ipotesi di partenza che viene riassunta con la convenzione dello stato di natura;

ii) V > P. Questa abbiamo visto essere realisticamente la condizione umana: la maggior parte degli individui, infatti, desidera più di quanto non possa nella vita di tutti i giorni;

iii) V = P. Questo è l'obbiettivo che si mira a raggiungere tramite il voto delle leggi nella società civile, quadrando per ciò il cerchio della politica. Ma, come intendere il passaggio da (i) a (iii)? Infatti, ci sono due modi opposti per raggiungere il predetto risultato: ora, aumentando il potere; ora, diminuendo le pretese dell'individuo, edulcorandone la volontà. Qual è la democrazia di Rousseau?

In terzo luogo, rimane del tutto insufficiente la trattazione dei poteri della iurisdictio, tanto più urgente, quanto più radicale il cambio di gubernaculum proposto. Di nuovo con le parole di Rousseau, "il patto sociale dà al corpo politico un potere assoluto su tutti quelli che sono le sue membra; ed è questo stesso potere che, diretto dalla volontà generale, porta, come ho detto, il nome di sovranità" (*op. cit.*, p. 44).

Quali, dunque, i rimedi per una sovranità popolare cosiffatta?

### 3.1.3. *La costituzione dei moderni*

Il terzo elemento che fa emergere l'evoluzione moderna del gubernaculum, dopo Locke e Rousseau, riguarda la nozione di costituzione. Il nuovo significato che il termine assume tra i moderni, rispetto alla tradizione antica e medioevale, può cogliersi nei seguenti cinque aspetti fondamentali.

In primo luogo, nella maggioranza dei casi la costituzione assume solenne forma scritta, al posto delle consuetudini tramandate da tempo immemore. L'unica eccezione di un certo rilievo è data, tuttora, dal sistema costituzionale britannico.

In secondo luogo, la costituzione dei moderni prevede una nuova responsabilità per gli atti di governo, che non soltanto interessa la sfera tradizionale della iurisdictio, ma si allarga al campo del gubernaculum. Quest'ultimo riposizionamento prende le forme della divisione dei poteri tra gli organi dello stato, come esposto da Locke nei *Due trattati sul governo* e, soprattutto, da Charles-Louis de Secondat, barone di Montesquieu (1689-1755), nella sua famosa opera *Lo spirito delle leggi* (1748).

In terzo luogo, la costituzione dei moderni è chiamata a contemperare i principi emersi con la filosofia politica e giuridica di Locke e di Rousseau, vale a dire le varianti liberali e democratiche del contrattualismo moderno. Come vedremo, le costituzioni dei moderni sono accompagnate da, o includono, un catalogo dei diritti naturali dell'uomo o, come diremmo oggi, dei diritti fondamentali costituzionalmente protetti.

In quarto luogo, il riposizionamento del gubernaculum con il riconoscimento dei diritti (naturali, universali, fondamentali, ecc.) del cittadino comporta la trasformazione stessa della iurisdictio. Alla tradizionale indipendenza dei giudici nei sistemi di common law, si aggiunge una nuova forma di giustizia costituzionale; prima, negli Stati Uniti d'America e, soltanto molto tempo dopo, in Europa e nel resto del mondo.

Infine, il vincolo di fedeltà e obbedienza che legava i sudditi alla persona politica e fisica del re, che tanti crucci aveva creato ancora a Locke, è sostituito dal vincolo di fedeltà e obbedienza alla Costituzione.

Altro elemento, poi, da avere ben presente riguarda il modo in cui è avvenuta complessivamente questa trasformazione. Più che di un passaggio o uno snodo, si è trattato di un mutamento che il più delle volte ha preso le forme del moto rivoluzionario. È questo il caso degli Stati Uniti d'America (1776), o della Francia (1789); oppure, si è trattato di un mutamento che è avvenuto a séguito degli effetti catastrofici di una guerra, come nel caso delle costituzioni tedesche di Weimar (1919) e di Bonn (1949), di quella odierna del Giappone (1946), o dell'Italia (1948).

In questa sede, prenderemo in considerazione il modello emerso negli Stati Uniti d'America sia perché, in fin dei conti, storicamente il primo, sia perché tuttora il più

longevo, sia perché particolarmente istruttivo al fine di cogliere la peculiarità degli odierni assetti istituzionali, nel passaggio dalle tradizionali forme di governo alla governance attuale. A questo punto, è opportuna una breve digressione che ha per oggetto la figura dei Padri fondatori statunitensi: dopo le avventure del gubernaculum, questa digressione servirà a introdurre l'analisi sulle sfide della iurisdictio.

### 3.1.3.1. *I Padri fondatori*

Li chiamano "padri fondatori" e non, come ad esempio in Italia, "costituenti", perché, quando avvenne il distacco dalla Madre patria britannica, l'idea dei patrioti non fu quella di ripartire daccapo, ridisegnando da zero le istituzioni, come sarebbe invece accaduto, a parole, con molti rivoluzionari francesi. Piuttosto, secondo un intento romantico che, in realtà, riconduce allo spirito protestante nordamericano, il proposito era di restaurare nel nuovo mondo il buon ordine antico, andato perduto nella corrotta Europa. È per questo che, andando per la prima volta a Washington, rimarreste sorpresi da alcune somiglianze architettoniche con l'antica Roma imperiale; è per questo che il Senato di quello stato si chiama così, nel ricordo di quello sul Tevere; è per questo che quello stato pullula di città e regioni come New York, New Hampshire, New Mexico e via discorrendo.

Dal punto di vista storico, il riferimento va alla crisi tra Madre patria e colonie britanniche sulla costa orientale dell'America del nord, occorsa tra gli anni sessanta e settanta del '700. Davanti alle pretesi fiscali del Parlamento britannico, capeggiato da William Pitt (1759-1806), i coloni eccepivano la violazione da parte degli inglesi delle Carte coloniali, ossia dei documenti ottriati dal re britannico, sulla cui base le prime colonie nordamericane si erano venute organizzando e auto-governando sin dal XVII secolo. Senza entrare nei dettagli giuridici della discussione (Pagallo 2002: 128-133), basti dire che la controversia di diritto finì per precipitare con lo scioglimento dell'Assemblea del Massachusetts e il pronunciamento rivoluzionario del Congresso americano del 15 maggio 1776 che, con la raccomandazione alle tredici Colonie di adottare costituzioni popolari, giunse alla dichiarazione della Virginia del 29 giugno 1776: "Il Governo di questo paese, quale precedentemente esercitato dalla Corona di Gran Bretagna, è interamente sciolto".

Dopo la vera e propria dichiarazione d'indipendenza a Filadelfia, il 4 luglio 1776, cui si accompagna la prima dichiarazione dei diritti universali dell'uomo, i rivoluzionari si doteranno di lì a poco di una loro propria Costituzione (1787), e di un'ulteriore Dichiarazione dei diritti (1791), introdotta con una serie di emendamenti alla medesima costituzione. Tra gli artefici della dichiarazione d'indipendenza e, in séguito, della costituzione – quelli che appunto saranno definiti "padri fondatori" – basti ricordare i più noti al lettore, come i primi due presidenti dell'Unione, George Washington (1732-1799) e John Adams (1735-1826), i tre autori del *Federalista*, ossia Alexander Hamilton (1755 o '57-1804), John Jay (1745-1829) e James Madison (1751-1836), nonché il genio di Benjamin Franklin (1706-1790) e del già menzionato Thomas Jefferson. Il quadro delineato da questa straordinaria generazione di statisti, politici, giuristi e scienziati, è a dir poco mirabile se, per la prima volta nella storia, si assiste alla formazione di uno stato fondato sui principi di sovranità popolare, riconoscimento dei diritti individuali, divisione dei poteri, federa-

lismo e tutela giurisdizionale costituzionale (e non solo ordinaria) dei diritti e dell'intero assetto istituzionale. In particolare:

i) sovranità popolare – secondo la raccomandazione del 15 maggio 1776, la nuova forma di sovranità alla quale s'ispirano gli Stati Uniti trova il proprio fondamento nel popolo: "We the People", come dichiara il preambolo della costituzione americana e come, più tardi, ripeterà tra gli altri il secondo comma del primo articolo della Costituzione repubblicana italiana. Non si tratta ancora, ad onor del vero, della democrazia preconizzata da Rousseau: eppure, verso gli anni venti dell'800, buona parte degli stati federati aveva introdotto il suffragio universale (per i maschi bianchi) che tanta meraviglia e ammirazione avrebbe in séguito suscitato nel pensatore francese Alexis de Tocqueville (1805-1859), come si evince dal suo fortunatissimo libro *Sulla democrazia in America* del 1835 (cinque anni dopo sarebbe stato pubblicato il secondo volume);

ii) riconoscimento dei diritti – stante la dichiarazione d'indipendenza del 1776, cui avrebbe fatto séguito la dichiarazione dei diritti dell'uomo e del cittadino in Francia nel 1789, il nuovo gubernaculum trova a proprio fondamento la concezione giusnaturalistica di Locke come limite alle decisioni dell'esecutivo o della maggioranza. Nella polemica tra federalisti contrari a una Carta dei diritti perché ridondante, e gli anti-federalisti favorevoli a tale carta perché sospettosi dei poteri di un governo fortemente centralizzato, prevalsero alla fine questi ultimi con la ricordata Dichiarazione dei diritti del 1791, ispirata da Jefferson e redatta da Madison;

iii) divisione dei poteri – come plasticamente scolpito dai primi tre articoli della costituzione del 1787 dedicati, rispettivamente, al legislativo, all'esecutivo e al giudiziario, si tratta di contrastare il potere con il potere; ma, rispetto alle teorizzazioni di Locke e Montesquieu, con due importanti novità. La prima, riguardante l'esecutivo, concerne la figura del Presidente della Repubblica a base elettiva e con mandato a termine, come tale opposto, non solo in forma simbolica, ai monarchi della vecchia Europa. La seconda, riguardante il potere giudiziario come componente essenziale dell'intero costrutto, prevede l'istituzione di una Corte suprema garante della Costituzione;

iv) struttura federale – per via della salutare diffidenza dei padri fondatori nei confronti dell'esercizio del potere, come testimoniato dal *Federalista*, il sistema di controlli e bilanciamenti stabilito sul piano degli organi centrali di governo viene integrato in chiave federale con la ripartizione di competenze tra detti organi e quelli degli Stati appartenenti all'Unione. Come nel caso della forma di stato repubblicana a base popolare, non si tratta di una novità assoluta, come dimostrato dal plurisecolare esempio della Svizzera. Ma, ancora una volta, per la prima volta nella storia si sperimentava simile impianto istituzionale su larga scala e, come detto a proposito della teoria delle reti (v. § 2.2.2), anche sul piano politico e giuridico, e non soltanto ingegneristico e fisico, la scala conta!

v) rigidità del costrutto – in virtù del disposto del quinto articolo della carta costituzionale, al fine di integrare o modificare la costituzione, era stabilita una procedura aggravata a maggioranze qualificate. Sebbene rimanesse aperta la questione su come dirimere l'eventuale contrasto tra costituzione e altre leggi dell'ordinamento, era fuor di dubbio la natura rigida, e non flessibile, della Carta, secondo una distinzione divenuta popolare in Europa soltanto nel secolo successivo;

vi) tutela giurisdizionale costituzionale – secondo quanto abbiamo visto essere un'altra novità assoluta del costrutto, al riposizionamento della formula del gubernaculum si pensa bene di aggiungere la ristrutturazione della iurisdictio. Alla tradizionale indipendenza della magistratura ordinaria tipica dei sistemi di common law, si aggiungono infatti le garanzie di una magistratura costituzionale sulla quale avremo modo di insistere nel prossimo paragrafo.

Tuttavia, dal punto di vista diacronico e, cioè, relativo alla dinamica di un sistema giuridico federale in espansione – per esempio, il Vermont venne ammesso nell'Unione nel 1791, il Kentucky nel 1792, …, la California, trentunesima, nel 1850, fino all'Alaska e alle Hawaii ammesse nel 1959, mentre il dibattito verte attualmente sull'isola di Puerto Rico come possibile cinquantunesimo stato – non deve sfuggire un fatto essenziale che, a sua volta, dà spunto a un parallelo suggestivo. Una volta che le tredici ex-Colonie che avevano dato origine al moto rivoluzionario ratificarono la Costituzione del 1787, sorgeva il problema d'immaginare la formula istituzionale e il tipo di relazione politica da adottare per la sterminata messe di territori che, a quel punto, si apriva verso Ovest. Ancora una volta in forma lungimirante e mirabile, la risposta di Jefferson e dei suoi contemporanei fu quella dell'auto-governo e dell'autonomia locale degli stati che, man mano, sarebbero andati formandosi e che, al momento opportuno, avrebbero potuto far richiesta di essere ammessi nell'Unione. Su queste basi, si è tracciata una similitudine tra le sfide pratiche e concettuali con le quali hanno dovuto confrontarsi Jefferson e la sua generazione, e i problemi sollevati al giorno d'oggi dalla disciplina della rivoluzione tecnologica e il cosiddetto cyberspazio. Poiché questi problemi saranno al centro della nostra attenzione nel paragrafo che conclude il presente capitolo, sembra opportuno indugiare sin d'ora sui termini del parallelismo. Così, è stato fatto notare che "il cyberspazio non è tale quale gli Stati Uniti occidentali del 1787, va da sé. Ma come gli Stati Uniti occidentali del 1787 si tratta (o, quanto meno, si è trattato) di una specie di spazio Jeffersoniano […] E come i territori dell'Ovest nel 1787, il cyberspazio solleva alcuni problemi difficili e richiede l'uso di alcune nuove idee, a proposito di governance, diritto, ordine e scala. Gli ingegneri ci hanno lasciato in eredità uno strumento notevole, impiegato per risolvere prodigiosi problemi tecnici associati con la comunicazione su scala globale. Il problema è quello che Jefferson e i suoi contemporanei hanno dovuto affrontare: come facciamo a mettere su delle istituzioni 'repubblicane' – istituzioni che rispettino la pari dignità degli individui e il loro diritto a partecipare nella formazione delle regole sotto cui vivono – a questo livello?" (Post 2009: 116-117).

## 3.2. *Le sfide della iurisdictio*

Per introdurre il tema di questo paragrafo sulle sfide della iurisdictio, conviene tornare alla figura della Corte suprema nordamericana. Fin qui, abbiamo fatto riferimento alla corte in tre occasioni: nel § 1.2, si è fatto cenno alle sue pronunce nei casi sul *Betamax* e sulla tecnologia P2P per sottolineare, contro ogni tecno-determinismo, il complesso intreccio tra gli effetti regolativi della tecnica, il diritto e la società.

Nel § 2.2.2.1, la ragione è dipesa da come i pareri e le opinioni maggioritarie della Corte si siano venuti disponendo spontaneamente nel corso dei secoli, secondo le leggi di potenza nei mondi piccoli degli ordini non intenzionali [1].

In questo capitolo (§ 3.1.3.1), infine, il richiamo ha avuto di mira le forme tradizionali della iurisdictio e come esse siano venute cambiando come l'altra faccia del riposizionamento del gubernaculum.

Qui, l'intento è piuttosto quello di evidenziare come funzioni questo ruolo di garanzia della iurisdictio che, specie in Europa, tanti malintesi ha provocato e provoca tuttora. Basti solo pensare alla famosa sentenza che la Corte suprema di Washington pronunciò il 24 febbraio 1803, nel caso *Marbury vs. Madison*, e al ruolo da protagonista svolto fin dal 1801 dal presidente della corte, John Marshall (1755-1835). Senza entrare nei dettagli della controversia che vedeva opporsi il Segretario di stato James Madison al giudice di pace William Marbury, la Corte definiva la questione nei termini di un conflitto tra leggi, ossia tra la legge ordinaria approvata dal Congresso nel 1789, il *Judiciary Act*, e la Costituzione. Sebbene il testo di quest'ultima, al ricordato articolo terzo, nulla prevedesse al riguardo, Marshall e la Corte giungevano alla conclusione che tale legge ordinaria dovesse essere dichiarata invalida, perché incostituzionale, in quanto, avendo prestato i giudici giuramento di fedeltà alla costituzione, essi erano sempre tenuti a rispettarla soprattutto nel caso di contrasto con altre leggi. A conforto della tesi, veniva richiamata la cosiddetta clausola di supremazia di cui all'articolo 6(2) della Costituzione, e l'ordine secondo il quale, prima, "questa Costituzione" e, poi, "le leggi degli Stati Uniti" e "i trattati" erano presentati come "la suprema Legge di questo Paese".

Ricapitolando, dalla pronuncia unanime (4 a 0) della Corte in *Marbury vs. Madison*, discendevano tre corollari fondamentali:

i) la Costituzione deve innanzitutto intendersi come sovraordinata a tutte le altre leggi e norme dell'ordinamento: essa rappresenta, cioè, la fonte delle fonti e, dunque, il metro di legalità per tutto il sistema giuridico considerato;

ii) spetta alla Corte suprema svolgere la funzione nomofilattica del sindacato di costituzionalità delle leggi – la *judicial review* statunitense – per cui, in caso di contrasto tra costituzione e altre leggi dell'ordinamento, queste ultime vanno dichiarate invalide;

iii) il potere di determinare questo eventuale contrasto tra fonti spetta anche ai giudici ordinari secondo un controllo diffuso di costituzionalità delle leggi che contrasta con il modello per lo più seguìto negli ordinamenti europei, dove viceversa vige un sindacato accentrato ad opera di un'apposita Corte costituzionale.

A séguito della sentenza non mancarono, come forse ovvio, critiche e perplessità, tra cui quelle del nostro Jefferson, divenuto nel frattempo il terzo presidente dell'Unione: ma, vuoi per la personalità di Marshall, vuoi per gli equilibri politici del paese, sia che la tesi della *judicial review* venisse intesa come un'interpretazione

[1] Nel caso in cui il lettore attento abbia notato che, in § 2.2.2.1, sulla scia di Fowler e Jeon, si è detto che le decisioni sotto esame comprendono l'arco temporale che va dal 1754 al 2002, mentre la Costituzione è del 1787, ciò dipende dal fatto che Fowler e Jeon hanno compreso anche i pareri maggioritari espressi dalla Corte suprema della Pennsylvania.

adeguata della costituzione, sia che venisse intesa come una sorta di fonte *extra* o *contra ordinem* dell'ordinamento, è su queste basi che sarebbe andata evolvendo la dialettica del sistema, tra gubernaculum e iurisdictio, nei secoli a venire.

Per contrasto, come diremo, il nuovo ruolo della iurisdictio rispetto all'ambito del gubernaculum, tra esecutivo e parlamento, sarebbe stato l'oggetto di un aspro dibattito, per molti versi ancora non sopito, in alcuni ordinamenti europei (si v. a continuazione § 3.2.1).

Inoltre, proprio nel vecchio continente, si assisterà a una ulteriore evoluzione della sfera della iurisdictio, stante il processo d'integrazione avviato a Parigi, nel 1951, con il Trattato costitutivo della Comunità europea del carbone e dell'acciaio (CECA) e, soprattutto, nel 1957 a Roma, con il Trattato istitutivo della Comunità economica europea (CEE) e quello sull'energia atomica (Euratom). Per via della dimensione o scala di questi processi (su cui § 3.2.2), la loro analisi consentirà di passare dalla tradizionale sfera degli ordinamenti incardinati sul principio di sovranità, all'esame degli odierni assetti istituzionali della governance (§ 3.3).

Passo dopo passo, vediamo di cosa si tratta.

### 3.2.1. *Le corti costituzionali in Europa*

Benché non sia stata certo la prima – *Una Corte costituzionale per l'Austria* di George Jellinek (1852-1911), ad esempio, risale al 1885 – la proposta di Hans Kelsen d'introdurre un sistema di giustizia costituzionale in Europa, che egli è venuto discutendo a partire dagli anni '20 e '30 del secolo scorso, ha rappresentato per lungo tempo il punto di riferimento indiscusso nel vecchio continente.

Rispetto al modello statunitense, Kelsen pensava in un primo momento a un ente di tipo legislativo, non giurisdizionale; a un organo centrale, più che a una tutela diffusa da parte dei giudici ordinari. La ragione dipendeva dal suo "monismo"; ossia, come detto (§ 2.1.2.2), l'idea di ricondurre tutte le fonti del sistema a un unico principio, seguendo in questo le tesi di un Hobbes o di un Rousseau. Tuttavia, a differenza del filosofo inglese e del francese, la novità consiste nel fatto che Kelsen non collega il principio di sovranità a un re o a una assemblea, come in Hobbes, sia pure in chiave democratica, come già in Rousseau. Piuttosto, a giudizio di Kelsen, avremmo dovuto concepire la costituzione come sovrana, secondo un principio liberal-democratico, e non più solo democratico, delle istituzioni, che ritroviamo del resto nel secondo comma del primo articolo della vigente costituzione italiana: "La sovranità appartiene al popolo che la esercita nelle forme e nei limiti previsti dalla costituzione". Ciò significa che nel caso, più che eventuale, di un possibile contrasto sul modo d'intendere tali "forme" e "limiti", le controversie tra maggioranza e minoranza avrebbero dovuto trovare composizione attraverso le decisioni di un apposito organo "in forma di tribunale" ma, appunto, con natura politica, più che puramente giuridica; e cioè come organo del potere legislativo, e non giurisdizionale (Kelsen ed. 1981).

Queste tesi trovarono in un pensatore a noi già noto (v. § 2.2), Carl Schmitt, il più scaltro e risoluto oppositore. A partire da *Il custode della Costituzione* (1931), la critica che egli svolge si snoda lungo un duplice piano: innanzitutto, anche a costo di negare l'evidenza, Schmitt attacca risolutamente chiunque avesse fatta propria la tesi della natura giurisdizionale di un tribunale costituzionale. Pensiamo a Jellinek,

che Schmitt cita, oppure, al Kelsen della *Teoria generale del diritto e dello stato* (1945), dove, nell'esaminare le "garanzie della costituzione", Kelsen delinea il tipo ideale di una corte della quale, mutando avviso, ne sottolinea il carattere giurisdizionale (*op. cit.*, ed. 1959: 159 e 272). Con le emblematiche parole di Schmitt, "la Corte suprema americana è tutt'altro che una corte costituzionale e la sua giurisdizione tutt'altro da ciò che oggi in Germania si suole indicare come giurisdizione costituzionale o statale" (Schmitt ed. 1981: 28).

Dopo di che, avendo riguardo al piano politico, sul quale aveva avuto modo d'insistere il primo Kelsen, Schmitt aveva buon gioco nel rifarsi all'allora diritto vigente – vale a dire la tragica costituzione della repubblica di Weimar che si sarebbe consegnata democraticamente a Hitler nel 1933 – per cui il Presidente del Reich, e non certo un tribunale, avrebbe dovuto dirimere i contrasti tra maggioranza e minoranza, e rappresentare il "custode della costituzione". In fin dei conti, il Presidente era eletto da tutto il popolo, aveva poteri di emergenza, poteva indire referendum e sciogliere la camera dei rappresentanti, sicché, a detta di Schmitt, era nella figura del capo dello stato che bisognava trovare "il punto centrale di un sistema plebiscitario come anche di funzioni ed istituzioni partiticamente neutrali" da contrapporre "al pluralismo dei gruppi di potere sociale economico e di difendere l'unità del popolo come totalità politica" (*op. cit.*).

Nonostante le tesi di Schmitt riconducano alle potenzialità eversive e totalitarie di una democrazia senza limiti, come nel caso di Rousseau (v. § 3.1.2), non manca ancora chi contrappone oggi le decisioni delle Corti costituzionali, quali organi di chiusura del sistema, alle decisioni degli organi democraticamente eletti nel seno delle istituzioni. A distanza d'oltre ottant'anni dal dibattito tra Schmitt e Kelsen, questi tribunali, sia pure con diversi criteri di competenza e composizione, sono stati tuttavia introdotti in pressoché tutti gli ordinamenti giuridici d'Occidente (ma non solo). Inoltre, il fatto che si sia consolidata nella prassi l'esperienza di organi di giustizia costituzionale mette bene in mostra l'originaria natura duale, più che monistica, delle istituzioni. Come chiarisce il caso emblematico della Corte suprema statunitense, questi organi chiudono sí il sistema, nel senso che spetta a loro definire "forme" e "limiti" secondo cui la sovranità popolare può essere legittimamente esercitata all'interno dell'ordinamento; ma, ecco il punto centrale della questione, che risale fino ai tempi di Henry de Bracton, tali poteri della iurisdictio sono pur sempre compatibili con l'esercizio di ciò che una volta erano definite le "prerogative" del gubernaculum e, oggi, rinviano alla sfera della discrezionalità politica degli organi rappresentativi della sovranità popolare. Sebbene non sia certo un caso che le istituzioni più longeve siano quelle che si sono rifatte a questo dualismo costitutivo tra gubernaculum e iurisdictio, ciò non significa che questo dualismo sia esente da problemi e da decisioni anche difficili: per rimanere agli Stati Uniti, basterebbe menzionare alcune sentenze della Corte suprema sia in tema di aborto (1973), sia su chi doveva essere il quarantatreesimo presidente dell'Unione, se cioè George W. Bush o Al Gore (2000); oppure se la riforma sanitaria del quarantaquattresimo, Barack Obama, fosse costituzionalmente legittima (2012).

Ma, lasciandoci alle spalle il dibattito tra Schmitt e Kelsen, occorre prestare attenzione al ruolo essenziale che la iurisdictio svolge nei confronti del gubernaculum e, soprattutto, come tale ruolo coinvolga l'ulteriore evoluzione interna della iurisdic-

tio stessa, per via della crescente complessità del sistema. Per chiarire questo duplice aspetto sarà il caso di prestare attenzione alle sfide della iurisdictio all'interno del processo d'integrazione europea.

### 3.2.2. *La competenza della competenza*

Per comprendere il vigente diritto costituzionale dell'Unione europea vale ciò che il diritto costituzionale nordamericano innanzitutto insegna: se si volesse intraprenderne lo studio, prescindendo dall'organo della iurisdictio, posto a chiusura del sistema, tale comprensione non sarebbe difficile, bensì, semplicemente impossibile.

Nel caso dell'Unione, il riferimento va alla Corte di giustizia di Lussemburgo, a far data dalla sentenza, richiamata all'inizio di questo capitolo, nel caso *van Gend & Loos* del 5 febbraio 1963 (n. 26 del 1962). In quell'occasione, la Corte, come detto, affermava che "la Comunità Economica Europea costituisce un ordinamento giuridico di nuovo genere nel campo del diritto internazionale" per due ragioni principali. La prima aveva a che fare con l'"applicabilità diretta" o "immediata" del Trattato istitutivo del 1957 e del complesso di norme che ne derivavano, nei limiti previsti da quello stesso trattato. Quest'ultimo, ai sensi dell'articolo 177, ne affidava appunto alla Corte di Lussemburgo l'interpretazione per così dire autentica, per cui, quale organo di chiusura del sistema, la Corte si comportava né più né meno come, sette anni prima, aveva fatto la Corte costituzionale italiana con la sua prima sentenza del 14 giugno 1956. Davanti alla novità, per la cultura giuridica italiana, di una costituzione rigida – e rispetto alla giurisprudenza della Corte di cassazione che si era peritata di distinguere tra una parte programmatica e una operativa dei disposti costituzionali – la Consulta stabiliva che i cosiddetti "programmi" della Carta fondamentale "vincolano immediatamente" il legislatore di Roma.

La seconda ragione per cui la CEE avrebbe rappresentato un inedito costrutto dipendeva dal fatto che, ancora una volta con le parole della Corte di giustizia, "il diritto comunitario, indipendentemente dalle norme emanate dagli Stati membri, nello stesso modo in cui impone ai singoli degli obblighi, attribuisce loro dei diritti soggettivi". A differenza, così, del diritto internazionale, in cui i diritti e gli obblighi degli individui non dipendono direttamente dagli accordi stipulati tra gli stati ma, bensì, dalla legge nazionale che dà esecuzione a quegli accordi sul piano interno, la Corte europea sanciva il principio dell'indipendenza e diretta applicabilità del diritto di cui è garante e custode, al fine di garantirne l'uniformità all'interno degli ordinamenti degli Stati membri.

Come corollario di questa duplice novità, alla diretta applicabilità dei regolamenti la Corte non soltanto avrebbe aggiunto di lì a poco quella di ulteriori disposizioni normative come le direttive a "efficacia diretta". Ma, fatto questo ancor più rilevante e rivoluzionario, i giudici di Lussemburgo arrivavano fino al punto di sentenziare nel caso *van Gend & Loos* che la CEE rappresentava un inedito nella storia del diritto internazionale, poiché si tratta di un ordinamento "a favore del quale gli Stati membri hanno rinunziato, se pure in settori limitati, ai loro poteri sovrani ed al quale sono soggetti non soltanto gli Stati membri, ma pure i loro cittadini".

Un anno dopo la pronuncia della Corte, la risposta arrivava significativamente, non già dall'ambito del gubernaculum, ma della iurisdictio. L'occasione sarebbe sta-

ta offerta dalla lite seguíta alla legge 1643, approvata dal Parlamento italiano il 6 dicembre 1962, con cui si provvedeva all'istituzione dell'ENEL, dando applicazione, per la prima e unica volta nella storia repubblicana, al disposto dell'articolo 43 della Costituzione. Quest'ultimo prevede, come noto, la legittima espropriazione d'imprese aventi "preminente interesse generale" e "che si riferiscano a servizi pubblici essenziali o a fonti di energia o a situazioni di monopolio". Il nuovo monopolio statale sull'energia elettrica finiva così per contrastare con le leggi sulla concorrenza dettate dal diritto comunitario e, per ciò, nella lite discussa davanti al giudice conciliatore di Milano, la causa finiva per approdare in Lussemburgo, stante il rinvio pregiudiziale alla Corte di giustizia per avere chiarimenti su come leggere le disposizioni del diritto europeo. D'altro canto, la questione veniva sottoposta anche al vaglio della Corte costituzionale di Roma ai sensi dell'articolo 134 della Costituzione, per decidere se la legge di nazionalizzazione dell'energia elettrica, pur legittima in base all'articolo 43 della Carta fondamentale, non ne avesse invece violato l'11. Si tratta dell'articolo che, dopo iniziali dubbi, era stato posto a fondamento della legittimità costituzionale del processo d'integrazione europea con la relativa rinuncia di sovranità nazionale da parte dell'Italia.

Nell'arco di quattro mesi, le due Corti giunsero a pareri opposti. Innanzitutto, il 7 marzo 1964, nel caso *Costa vs. Enel*, la Consulta di Roma salvava l'ENEL, adducendo che la legge con cui il Parlamento italiano aveva recepito i trattati comunitari, ossia la legge n. 1203 del 14 ottobre 1957, era pur sempre una legge ordinaria e, come tale, l'articolo 11 della Costituzione non avrebbe conferito alla legge 1203 un'efficacia superiore a quella propria di tale fonte del diritto. Con le parole della Corte, "non vale l'argomento secondo cui lo Stato, una volta che abbia fatto adesioni a limitazioni della propria sovranità, ove volesse riprendere la sua libertà d'azione, non potrebbe evitare che la legge, con cui tale atteggiamento si concreta, incorra nel vizio d'incostituzionalità. Contro tale tesi stanno le considerazioni ora esposte, le quali conducono a ritenere che la violazione del Trattato, se importa responsabilità dello Stato sul piano internazionale, non toglie alla legge con esso in contrasto la sua piena efficacia". In altre parole, avrebbe dovuto valere il criterio ordinario per risolvere l'antinomia delle leggi, ossia il criterio cronologico stante il quale vale "il principio della successione delle leggi nel tempo", per cui, nel caso di specie, era fatta salva l'istituzione dell'ENEL (legge del dicembre 1962) con buona pace della CEE (legge dell'ottobre 1957).

Il 15 luglio di quello stesso anno, 1964, arrivava la risposta dal Lussemburgo: i giudici della Corte di giustizia prendevano spunto dal caso *Edison*, già *Costa vs. ENEL*, per ribadire non solo il principio emerso nel precedente caso *van Gend & Loos*; vale a dire, l'applicabilità diretta o immediata del Trattato di Roma, come anche, in parte, della normativa comunitaria da esso derivata. Ma, appunto perché, con la ratifica del trattato, gli stati membri della CEE avrebbero "definitivamente" rinunciato alla propria sovranità – beninteso, relativamente all'ambito delle competenze giuridiche comunitarie – il risultato era che da questa stessa rinuncia ne seguiva, ad avviso della Corte di giustizia, il "primato del diritto comunitario" in quella medesima sfera normativa. Alle competenze legislative e giurisdizionali previste dalla Costituzione italiana del 1948, in altri termini, avrebbero dovuto subentrare, in ragione delle stesse "limitazioni di sovranità" stabilite dal suo articolo 11, le compe-

tenze istituite dal Trattato di Roma che includono, tra le altre cose, proprio la riserva in favore della Corte di giustizia di Lussemburgo come organo di chiusura del sistema.

La Corte costituzionale italiana, poco alla volta e sia pure nell'arco di vent'anni, sarebbe tornata sui propri passi. Il 30 ottobre 1975, nel caso *Industrie chimiche Italia centrale*, con la sentenza 232, la Consulta ammetteva che "la successiva emanazione di norme legislative interne, anche se aventi lo stesso contenuto sostanziale dei regolamenti comunitari, comporta non soltanto la possibilità di differirne, in tutto o in parte, l'applicazione, in aperto contrasto con l'art. 189, secondo comma, del Trattato di Roma, ma anche una ben più grave conseguenza, in quanto la trasformazione del diritto comunitario in diritto interno ne sottrae l'interpretazione in via definitiva alla Corte di giustizia delle Comunità, con palese violazione del regime stabilito dall'art. 177 dello stesso trattato quale necessaria e fondamentale garanzia d'uniformità in tutti gli Stati membri". Inoltre, proseguiva l'argomentazione della corte, non poteva certo riconoscersi al giudice ordinario il potere di disapplicare le disposizioni nazionali in contrasto con la normativa comunitaria, in quanto ciò "equivarrebbe ad ammettere il suo potere di accertare e dichiarare una incompetenza assoluta del nostro legislatore, potere che nel vigente ordinamento sicuramente non gli è attribuito". Su queste basi e in ragione di un intricato sentiero interpretativo che in questa sede possiamo tralasciare, la Consulta finiva così, in un primo momento, per creare una nuova ipotesi di ricorso ai sensi dell'articolo 134 della Costituzione, nel senso che la legge nazionale in conflitto con la normativa comunitaria avrebbe potuto essere rimossa solo attraverso la dichiarazione d'illegittimità costituzionale. Dopo di che, seguendo quanto la Corte di giustizia aveva sentenziato il 9 marzo 1978, nel caso *Simmenthal*, la Consulta cambiava nuovamente idea l'8 giugno 1984. Con la sentenza 170 del caso *Granital*, si riconosceva infatti il potere dei giudici italiani, in caso di contrasto tra le due normative, di decidere la controversia direttamente sulla base delle disposizioni del diritto comunitario, disapplicando pertanto il diritto nazionale. Ancora una volta con le parole della corte, "il regolamento comunitario va, dunque, sempre applicato, sia che segua, sia che preceda nel tempo le leggi ordinarie con esso incompatibili: e il giudice nazionale investito della relativa applicazione potrà giovarsi dell'ausilio che gli offre lo strumento della questione pregiudiziale di interpretazione, ai sensi dell'art. 177 del Trattato. Solo così è soddisfatta la fondamentale esigenza di certezza giuridica".

Il risultato di questo capovolgimento giurisprudenziale è stato duplice: per un verso, da più di trent'anni in Italia si è stabilito un doppio binario di controllo sulla legittimità delle leggi da parte dei giudici ordinari. Questi ultimi, infatti, quando appurano la non manifesta infondatezza del contrasto tra costituzione e leggi del parlamento di Roma devono, ai sensi dell'articolo 134 della Carta fondamentale, rinviare gli atti alla Consulta secondo il sindacato accentrato già caro a Kelsen. Ma, quando si discuta dell'eventuale contrasto tra leggi del parlamento e normativa europea, subentra un sindacato diffuso di legittimità, né più né meno come nella tradizione costituzionale statunitense, salvo che, in casi di dubbi, il giudice ordinario ritenga di ricorrere al rinvio pregiudiziale alla Corte di giustizia di Lussemburgo.

D'altro canto, per un problema risolto, ce n'è un altro che si è aperto e che concerne l'ipotesi in cui il diritto europeo, sovraordinato alla normativa nazionale, fini-

sca tuttavia per violare principi supremi e irrinunciabili della costituzione di uno stato membro. Sebbene l'ipotesi, almeno per il momento, sia rimasta fortunatamente tale, questo è il punto sollevato sia dalla Consulta con la sentenza 183 del 27 dicembre 1973 nel caso *Frontini*, sia dal Tribunale costituzionale tedesco, a partire dalla pronuncia del 29 maggio 1974, nel caso *Solange*. La questione viene spesso riassunta come un problema di "competenza della competenza", nel senso che, se è vero che gli stati membri rinunciano definitivamente a proprie quote di sovranità tramite i trattati, è altrettanto innegabile che le competenze dell'Unione europea non sono "originarie" bensì "derivate", avendo la propria fonte nelle cessioni di sovranità formalizzate con quei trattati. Nel caso di conflitto sull'estensione di tale rinuncia alla sovranità a chi spetta l'ultima parola? Alla Corte di giustizia di Lussemburgo quale depositaria del significato da attribuire alla lettera e spirito dei trattati europei, o alle Corti nazionali quali custodi dei valori irrinunciabili delle proprie Carte fondamentali?

## 3.3. *L'odierno reticolo istituzionale*

Alla luce delle precedenti osservazioni sul processo d'integrazione europea, possiamo far ritorno alla figura 14 con la quale abbiamo aperto il presente capitolo. Integrando questa con la figura 5 del capitolo secondo, otteniamo i nuovi osservabili e variabili dell'analisi:

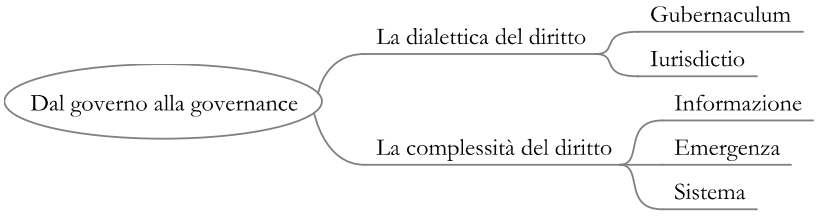


Figura 15: *L'odierno reticolo istituzionale*

Sul primo fronte della nuova figura, il processo d'integrazione europea ha chiarito la tensione duale dell'ordinamento tra gubernaculum e iurisdictio. Per un verso, si tratta del percorso caro alle versioni monistiche dell'ordinamento, secondo la direzione che va dal gubernaculum alla iurisdictio, vale a dire dalle regole stabilite ora dal potere legislativo ora dall'esecutivo, agli organi della giurisdizione che sono tenuti ad applicare dette norme in omaggio al principio di legalità e lo stato di diritto. D'altra parte, però, occorre sempre ricordare il movimento inverso che va dalla iurisdictio al gubernaculum, sia pure nel rispetto della sfera di discrezionalità che spetta agli organi rappresentativi della sovranità popolare. Tornando alle questioni della "competenza della competenza" emerse nello scorso paragrafo, basti far cenno alla serie di decisioni prese dal Tribunale costituzionale federale tedesco sulla compatibilità dei trattati europei con i principi irrinunciabili previsti dalla carta fondamentale di quello stato membro. Ad esempio, il 12 ottobre 1993, con la sentenza con la

quale la Corte tedesca si pronunciava sulla legittimità costituzionale del Trattato di Maastricht – che prevedeva, tra le altre cose, la rinuncia tedesca alla propria sovranità monetaria e, dunque, la sostituzione del marco tedesco con l'istituendo euro – i giudici di Karlsruhe finivano per ammettere la legittimità degli accordi; ma, ecco il punto, sulla base di un nutrito elenco di riserve e condizioni. Con ciò che a buon diritto può essere reso con gergo giuridico italiano come "sentenza monito", la Corte fissava una serie di contro-limiti al processo d'integrazione europea, in ragione del principio democratico e della tutela dei diritti fondamentali garantiti dalla costituzione tedesca, che sarebbero stati in séguito ripresi quasi alla lettera dal Trattato di Amsterdam (sottoscritto da tutti gli stati membri il 2 ottobre 1997, ed entrato in vigore il primo maggio 1999).

Sul secondo fronte della figura 15, il processo d'integrazione europea rende bene il passaggio dalle tradizionali forme di governo all'odierno sistema della governance, dato che gli organi del gubernaculum su scala nazionale sono stati affiancati, integrati o, perfino, sostituiti da un più vasto e complesso reticolo istituzionale. La ragione più appariscente del processo è certamente sistemica, nel senso che i problemi con i quali sono chiamati a misurarsi gli stati membri sono tali che essi, presi singolarmente, non sarebbero in grado di affrontarli adeguatamente: è il caso della conservazione delle risorse biologiche e dell'ambiente, con la tutela dei consumatori nel mercato globale o con la protezione dei dati personali. Tuttavia, la natura di questi problemi non può che riportare al dato informativo sull'identità dell'Unione e al dissidio tra le corti su come intenderne il costrutto. Tralasciando i bizantinismi delle diverse istituzioni, per cui anche al più agguerrito degli studenti di giurisprudenza può sfuggire la sottile differenza, che pur esiste, tra il Consiglio europeo, il Consiglio dell'Unione europea e il Consiglio d'Europa, è sufficiente ricordare come alla tesi della Corte di Lussemburgo che vede nel diritto europeo un ordinamento di nuovo genere nel campo del diritto internazionale, si contrappone chi, come la Corte di Karlsruhe, ritiene invece che l'Unione "è basata sulle autorizzazioni di Stati che rimangono sovrani, agendo nell'ambito internazionale regolarmente tramite i loro Governi e dirigendo così l'integrazione".

A questi nodi si aggiungano, inoltre, i mai sopiti problemi relativi al cosiddetto deficit democratico delle istituzioni che hanno, fin qui, trovato un fragile equilibrio nel principio di sussidiarietà. Secondo l'articolo 5.3 del trattato sull'Unione, dopo le modifiche introdotte dal trattato di Lisbona il 13 dicembre 2007, entrato poi in vigore il primo dicembre 2009, "in virtù del principio di sussidiarietà, nei settori che non sono di sua competenza esclusiva l'Unione interviene soltanto se e in quanto gli obiettivi dell'azione prevista non possono essere conseguiti in misura sufficiente dagli Stati membri, né a livello centrale né a livello regionale e locale, ma possono, a motivo della portata o degli effetti dell'azione in questione, essere conseguiti meglio a livello di Unione". In altre parole, l'intervento europeo si legittima sul piano del gubernaculum, più che della iurisdictio, in ragione della ricordata complessità sistemica di problemi che investono gli stati membri nel loro insieme e, rispetto ai quali, questi ultimi non appaiono all'altezza del compito. Oltre alle competenze esclusive della Unione in materia d'unione doganale, conservazione delle risorse biologiche o alle regole sulla concorrenza necessarie al mercato interno, si pensi, ai sensi dell'articolo 4 del trattato sul funzionamento dell'Unione, alla "competenza

concorrente" riguardo la coesione economica, sociale e territoriale, la pesca e l'agricoltura, l'ambiente, l'energia o i trasporti. La complessità sistemica che legittima in questi casi il gubernaculum dell'Unione, quando cioè è dimostrabile che gli effetti dell'azione possano "essere conseguiti meglio a livello d'Unione", suggerisce una competenza tecnocratica fondata sul suo saper fare che, proprio per questo, lascia però irrisolti i nodi dai quali siamo partiti, ossia quelli relativi all'identità del costrutto e al suo deficit democratico.

Del resto, i problemi non mancano anche per la tradizionale scala nazionale del gubernaculum, diventato spesso, a sua volta, sovradimensionato rispetto alle sfide della società complessa. Il riferimento va alle difficoltà cui, in questo caso, è andato incontro l'apparato amministrativo pubblico degli stati nazionali, secondo una crisi sempre più accentuata a partire dagli anni ottanta del secolo scorso che, non a caso, ha visto l'opacità e proverbiale lentezza degli organi burocratici soppiantata da nuove forme di partenariato pubblico e privato (PPP), con ondate di privatizzazioni, devoluzioni e volontariato che fanno da controcanto ai processi di aggregazione sovranazionale ricordati in precedenza. Le variabili del secondo osservabile nel passaggio dalle tradizionali forme di governo all'odierna governance, ossia i profili dell'informazione, emergenza del kosmos e complessità sistemica, riappaiono di qui in maniera eguale e contraria a quanto visto in precedenza:

i) dal punto di vista del sistema i problemi sono complessi perché lo investono nel suo insieme, ma questo insieme può essere sottordinato alla scala dello stato. Significativamente, alcuni ordinamenti, come quello italiano, hanno inserito nella propria carta costituzionale il principio di sussidiarietà ma, appunto, in funzione eguale e contraria al ruolo svolto da tale principio su scala europea;

ii) dalla complessità dei fenomeni possono emergere forme d'ordine spontaneo che garantiscono una maggiore efficienza rispetto all'intervento dello stato: "il potere e l'azione dello stato sono ora dispersi in una miriade di reticoli spazialmente e funzionalmente distinti, che consistono di ogni tipo di organizzazioni pubbliche, private e di volontariato" (Bevir 2012: 67);

iii) la formula con cui, più spesso, si riassume questa trasformazione del ruolo e funzioni svolte dallo stato è quella della governance, a suggerire ancora una volta come il tradizionale ambito del governo sia stato affiancato, integrato o, perfino, sostituito, questa volta "verso il basso", da un più vasto e complesso reticolo di associazioni non governative (NGO), partenariati, cooperative, e via discorrendo. Si può ripensare in questo modo al ruolo che lo stato svolge come una meta-governance, nel senso di provvedere al coordinamento di questa stessa governance: "ciò suggerisce che lo stato dipenda in forma crescente dalla negoziazione, diplomazia, e strumenti informali di indirizzo. Lo stato indirizza e regola in forma crescente insiemi di organizzazioni complesse, di governo locale e reti, piuttosto che fornire direttamente i servizi tramite il proprio apparato burocratico" (Bevir 2012: 75).

Tuttavia, riferendoci a questo punto della nostra riflessione alla nozione di governance per indicare tanto i nuovi assetti istituzionali che si dislocano sopra lo stato, quanto al suo interno, non corriamo il rischio di svuotare il concetto della sua funzione euristica? Non faremmo la fine occorsa al mitico esploratore scozzese David Livingstone (1813-1873), per cui, nelle peripezie tra lo Zambesi e il Nilo, il fatto

che egli fosse da qualche parte nel continente africano era un dato assodato; ma dove, precisamente, egli fosse rimaneva pur sempre un mistero?

È giunto il tempo per qualche definizione.

### 3.3.1. *I settori della governance*

La fortuna conosciuta dal termine "governance" dipende dalla circostanza che designa, indifferentemente, la forma in cui l'interazione sociale è organizzata o si coordina, ora, sul piano politico, tradizionalmente imperniato sul concetto di autorità; ora, sul piano economico, fondato sul principio della domanda e dell'offerta con il criterio regolativo dei prezzi in un mercato; ora, sul piano dell'interazione sociale, che fa leva invece sui rapporti di fiducia. Da questa versatilità del termine si comprende come esso sia stato impiegato nei più svariati settori della ricerca, per mettere a fuoco sia forme di organizzazione politica come la governance regolativa, partecipativa o collaborativa; sia forme di organizzazione economica come la governance aziendale o d'impresa; sia forme di organizzazione sociale come nel caso della governance non-profit.

L'uso del termine può inoltre servire a illustrare le questioni interdisciplinari di un determinato ambito. Oltre all'esempio della governance europea, sul quale ci siamo soffermati nei paragrafi precedenti, si pensi al caso della governance delle tecnologie dell'informazione, dell'ambiente, o d'internet, su cui avremo peraltro modo di soffermarci nel prosieguo del volume (si v. infatti § 3.4).

Tuttavia, in questa sede, avendo a che fare con l'evoluzione degli ordinamenti giuridici contemporanei, conviene restringere il fuoco dell'analisi e approfondire la nozione dal punto di vista del diritto. A partire dal discorso inaugurale tenuto da Kofi Annan nel luglio 1997, quale nuovo segretario generale dell'ONU, il termine governance è stato al centro del dibattito che si è aperto presso alcune organizzazioni internazionali, come le stesse Nazioni Unite (ONU), il Fondo Monetario Internazionale (FMI) e la Banca Mondiale. Qui, il fine è stato di precisare come gli organi di governo su scala nazionale siano stati accompagnati o, perfino, soppiantati da un più vasto e complesso reticolo istituzionale. Ad esempio, secondo la Banca Mondiale, l'idea di governance concerne "il processo e le istituzioni attraverso le quali le decisioni sono prese e l'autorità viene esercitata in un paese" (in Grindle 2007: 556). Altri fanno riferimento all'"esercizio dell'autorità attraverso tradizioni e istituzioni, sia formali sia informali, volte al bene comune" (Kaufmann 2003: 5). Altri ancora, come Hyden, Court e Mease, prestano attenzione alla "formazione e gestione delle regole, sia formali sia informali, che disciplinano lo spazio pubblico, ambito entro il quale lo stato, insieme ad altri attori economici e sociali, interagiscono per prendere decisioni" (in Grindle 2007: 557).

Su queste basi, la nozione è stata ulteriormente raffinata nei termini di "buona governance". Con la Banca Mondiale, l'accento è stato così posto sulle nozioni di responsabilità e apertura delle istituzioni in tre aree cruciali, riguardanti la "selezione, responsabilità e ricambio delle autorità", "l'efficienza delle istituzioni, del sistema normativo e delle risorse organizzative", nonché il "rispetto per le istituzioni, le leggi e l'interazione tra gli attori nella società civile, gli affari e la politica" (*ibidem*). Nel caso di Hyden, Court e Mease, la nozione di buona governance deve invece es-

sere colta lungo sei diverse dimensioni, definite dalla "partecipazione, correttezza, moralità, efficienza, responsabilità e trasparenza", in ciascuna delle seguenti aree: "società civile, politica, governo, burocrazia, economia e magistratura" (*ibidem*). A sua volta, per Kaufmann, tali dimensioni hanno piuttosto a che fare con il diritto di "parola e responsabilità esterna, stabilità politica e assenza di violenza, di criminalità e terrorismo, effettività di governo, assenza di gravami regolatori, stato di diritto e controllo della corruzione" (Kaufmann 2003: 5). Queste definizioni tornano in parte con l'FMI: se, da un lato, i due obiettivi della governance dovrebbero essere di "migliorare la gestione delle risorse pubbliche" e "sostenere lo sviluppo e mantenimento di uno stabile e trasparente ambiente economico e regolativo, per contribuire all'efficienza delle attività del settore privato", la buona governance consiste a sua volta nel garantire "lo stato di diritto, migliorando l'efficienza e responsabilità del settore pubblico, e contrastando la corruzione" (in Grindle 2007: 556).

In ragione di questo quadro generale, non sorprende che alcuni studiosi abbiano criticato la lunghezza dei programmi d'intervento suggeriti dall'ONU, dall'FMI, o dalla Banca Mondiale, al fine di favorire lo sviluppo politico ed economico degli stati in nome della "buona governance". Piuttosto, bisognerebbe stabilire la lista di problemi che dovrebbero avere la priorità, a seconda del contesto esaminato e le condizioni specifiche di ogni paese (Grindle 2005: 1).

Riprendendo il suggerimento metodologico, quali, dunque, sono le questioni cui occorre assegnare la priorità, per capire i nodi giuridici del passaggio dalle tradizionali forme di governo a quelle odierne della governance?

### 3.3.2. *I livelli della governance*

La prima e fondamentale distinzione che occorre aver presente, affrontando gli odierni temi della governance e della buona governance, concerne i piani locale e globale della stessa, là dove il tradizionale livello del governo statale, sul doppio fronte del gubernaculum e della iurisdictio, rappresenterebbe lo snodo o collegamento tra i due piani d'indagine. Sebbene, come detto (v. § 3.3), tanto il livello sovranazionale quanto quello interno della governance degli stati debbano affrontare le medesime sfide della complessità – nei termini già visti del diritto come informazione, come emergenza degli ordini spontanei e secondo la nuova scala, o dimensione strutturale o sistemica, dei problemi da affrontare – esiste pur tuttavia una differenza di fondo.

Sul piano interno alla governance degli stati, la lunga lista degli esperti dell'ONU, dell'FMI o della Banca Mondiale, può essere convenientemente affrontata con il bagaglio dei concetti e criteri messi a punto dalla tradizione filosofica giuridica e politica moderna, a proposito delle modalità in cui "le decisioni sono prese e l'autorità viene esercitata in un paese" (Banca Mondiale), sia pure con strumenti informali per l'"esercizio dell'autorità" (Kaufmann), e in rapporto "ad altri attori economici e sociali" (Hyden, Court e Mease). Si tratta di un plesso di problemi che, potendo astrattamente fare a meno dei fenomeni di crescente interdipendenza mondiale, sono intellegibili con le lenti concettuali messe a disposizione dal contrattualismo, dal federalismo, dal costituzionalismo, con lo stato di diritto, la sussidiarietà, e via dicendo.

È piuttosto sul piano globale della governance che si profilano le difficoltà di affrontare questi temi nei consueti termini della legittimità democratica delle istituzioni, della trasparenza con cui le decisioni sono prese, della responsabilità politica e giuridica dei diversi organi statali e non statali, che si danno in rapporto al ruolo di altri attori economici e sociali. Prova ne sia il dibattito tra "globalisti" e "realisti" sulle sorti dell'ordinamento giuridico internazionale, per cui, da un lato, sulle orme del progetto cosmopolitico di Kant (v. § 1.1.3), messo a punto nel saggio *Per la pace perpetua* (1795), è maturata la convinzione che per rispondere alle sfide dell'ordine mondiale occorra istituire una sorta di costituzione democratica su scala globale, con la quale far fronte allo stato di natura tra stati sovrani preconizzato da Hobbes (v. § 2.1.2.1). Al fine di pensare a "un nuovo ordinamento mondiale di tipo universalistico" come quello vagheggiato dal filosofo tedesco Jürgen Habermas (n. 1929), bisognerebbe partire da qui per colmare l'"assenza del terzo" che, a giudizio di Hobbes, segna la differenza tra ordine nazionale e disordine internazionale. Con le parole del filosofo italiano Norberto Bobbio (1909-2004), "il Terzo superiore alle parti per essere efficace senza essere oppressivo deve disporre di un potere democratico, ovvero fondato sul consenso e sul controllo delle stesse parti di cui deve dirimere il conflitto" (Bobbio 1989: 8-9). Tuttavia, anche ad ammettere che lo spettro della soggettività internazionale sia venuto allargandosi a organizzazioni non governative e, in prospettiva, a ogni individuo come cittadino del mondo, rimangono, a dir poco, problemi sia fattuali sia teorici, sul modo d'intendere questo Terzo mondiale. Lasciando per il momento in sospeso il giudizio sull'odierno stato di salute del diritto internazionale e di organizzazioni come l'ONU, l'FMI o la Banca Mondiale, a che titolo è lecito proporre su scala planetaria un modello di gubernaculum che, come visto (§ 3.3), non gode di ottima salute nemmeno in casa propria?

D'altro canto, sul fronte dei teorici realisti, è stato a vario titolo contestata la tesi che, in mancanza di un terzo mondiale, segua necessariamente, al modo di Hobbes, lo stato di natura. All'idea di chi continua a vedere nelle norme secondarie o di organizzazione del diritto internazionale una sorta di mera moralità internazionale sottoposta, peraltro, al proprio interesse vitale (v. ancora § 2.1.2.1), si contrappone la tesi di quanti sostengono che l'interdipendenza sistemica tra singoli stati fa emergere una condizione di "governance senza government" (Rosenau e Czempiel 1992), ovvero una sorta di "anarchia cooperativa" tra stati (Bull 1977), oppure un "ordine anarchico" delle relazioni internazionali (Waltz 1987). Anche a concedere ai teorici del realismo l'emersione di queste forme d'ordine spontaneo, tuttavia, sia pure in forma eguale e contraria alle tesi dei globalisti, rimangono una messe di problemi aperti. Come detto a proposito di un cultore degli ordini spontanei come Hayek (v. § 2.2.1), non soltanto questi ordini possono condurre a vicoli ciechi; ma, davanti ad essi, c'è bisogno di un approccio normativo che, nondimeno, nei realisti per lo più manca.

Per chiarire ulteriormente il dilemma tra una teoria senza prassi e una prassi priva di vincoli normativi, valga a continuazione l'esempio forse più probante dell'odierna governance, vale a dire quella globale d'internet (§ 3.4). Illustrati i termini della questione con il tradizionale rapporto tra gubernaculum e iurisdictio (§ 3.4.1), nonché con l'odierno reticolo di attori privati e organismi pubblici (§ 3.4.2), l'intento è di mettere in mostra i limiti che affliggono le analisi, sia dei globalisti sia

dei realisti, alla luce dei problemi tuttora aperti nel mondo della rete (§ 3.4.3). Alla prassi più rigogliosa degli ordinamenti giuridici contemporanei farà da controcanto una teoria con tre criteri normativi, e cioè tre modi in cui è dato stabilire ciò che si può o non si deve fare nella governance d'internet.

## 3.4. *La governance di internet*

Possiamo riassumere quanto fin qui detto a proposito di tecnologia, complessità e diritto, proprio in relazione al tema del governo della rete.

Rispetto ai motivi del capitolo primo, internet rappresenta infatti, per molti versi, l'emblema della rivoluzione tecnologica in corso. La rete (delle reti) costituisce il tessuto nervoso degli odierni sistemi sociali, da cui dipende una parte rilevante dei commerci e il progresso economico, l'istruzione e la comunicazione, la difesa e la sicurezza degli stati, la libertà di parola e la garanzia della privacy personale, fino al banale intrattenimento degli individui. A proposito della quarta rivoluzione, abbiamo già detto del modo in cui internet possa incidere sui processi cognitivi del diritto (§ 1.4.1), sui suoi istituti (§ 1.4.2), tecniche (§ 1.4.3), e istituzioni (§ 1.4.4), riassumendo questi processi con la formula del diritto nell'era delle società ICT-dipendenti.

Rispetto ai temi del capitolo secondo, internet compendia i tre livelli in cui è dato osservare la complessità giuridica dell'odierna rivoluzione tecnologica. In primo luogo, internet mette in chiaro i termini del diritto come informazione, là dove ha trasformato vecchi istituti giuridici, come la privacy o la tutela del diritto d'autore, nella questione di come avere a disposizione o tenere sotto controllo il flusso d'informazioni in rete. In secondo luogo, internet è il caso più lampante di come emergano dalla complessità forme spontanee d'ordine, secondo quanto approfondito nel caso dei "mondi piccoli" della rete (§ 2.2.2.1). In terzo luogo, a proposito dei rischi del sistema, internet spiega perché le nostre società siano propriamente complesse, nel senso che i problemi con cui devono misurarsi investono dette società nel loro insieme (§ 2.3).

Infine, rispetto ai temi del presente capitolo, internet mette bene in mostra il passaggio occorso dalle forme tradizionali di governo ai temi attuali della governance. Da un lato, sul fronte del gubernaculum, si è avuto fin qui il modo di ricordare il profluvio di leggi con cui i legislatori nazionali e internazionali hanno reagito all'impatto tecnologico sul diritto, nei settori del diritto penale, del copyright, ecc. (§ 1.4.2-3). D'altro canto, si tratta di completare questa serie d'interventi sul fronte del gubernaculum, considerando a continuazione le risposte nel frattempo emerse sul piano della iurisdictio (§ 3.4.1). Avendo a mente il dibattito tra globalisti e realisti, cui si è fatto cenno in precedenza, lo scopo che ci si propone con l'analisi dei prossimi paragrafi, è duplice. Rispetto alle tesi dei globalisti alla ricerca di un terzo mondiale, il fine è di apprezzare pienamente la complessità della governance d'internet, mostrando come l'insieme istituzionale d'organi pubblici, nazionali e internazionali, costituisca solo una parte, e in molti casi neanche quella più rilevante, di un ben più intricato reticolo di attori e società privati, organizzazioni civili, e forme d'ordine spontaneo (§ 3.4.2). Rispetto agli assunti dei teorici del realismo, occorrerà invece fornire una serie di criteri normativi con i quali posizionarsi rispetto ai pro-

blemi che pur non mancano (§ 3.4.3), nei termini dell'onere della prova (§ 3.4.3.1), dovere di conoscenza (§ 3.4.3.2), e scelta degli strumenti giuridici con i quali far fronte a dette questioni (§ 3.4.3.3). Su queste basi, saremo in grado di formalizzare le fonti giuridiche delle società ICT-dipendenti nel capitolo quarto.

### 3.4.1. *Tra gubernaculum e iurisdictio*

In ragione della dialettica del diritto e del dualismo costitutivo nelle istituzioni, tra gubernaculum e iurisdictio, non sorprenderà che gli organi giurisdizionali, al pari di quelli di governo, si siano venuti occupando ben presto dei problemi giuridici di internet. In linea generale, possono darsi tre scenari differenti:

i) gli organi della iurisdictio possono essere chiamati a sindacare la legittimità delle scelte politiche prese dagli organi del gubernaculum;
ii) la questione può vertere su problemi che tali scelte politiche, fissate in una legge o in uno statuto, hanno lasciato aperti;
iii) gli organi della iurisdictio possono ritrovarsi a decidere controversie su cui il legislatore non ha saputo, o non ha voluto, intervenire.

In questa sede, concentreremo l'attenzione su due decisioni della Corte suprema nordamericana e della Corte di giustizia di Lussemburgo, sia perché esse appaiono di per sé particolarmente interessanti, sia perché utili per il prosieguo della nostra riflessione.

Il primo caso, deciso dalla Corte suprema, ha a che fare con il primo dei tre scenari ora menzionati, ossia il sindacato di legittimità costituzionale delle leggi ordinarie. La normativa in esame riguardava alcune disposizioni del *Communications Decency Act* che il Congresso statunitense aveva approvato il primo febbraio 1996, al fine di impedire e sanzionare la messa a disposizione sulla rete di materiale "indecente" e "chiaramente offensivo". Come avrebbe poi spiegato il Governo davanti alla Corte suprema, le misure sarebbero state rese necessarie dal dilagare della pornografia in rete, ciò che avrebbe "indotto innumerevoli cittadini ad allontanarsi dal mezzo per via del rischio di esporre se stessi e i propri figli a materiale dannoso". Il parametro di costituzionalità da avere presente, riporta al primo degli emendamenti alla Costituzione introdotti nel 1791 (v. § 3.1.3.1). Si tratta del diritto che forse sta più a cuore agli americani: "Il Congresso non potrà fare leggi riguardo alla istituzione di una religione, o per proibirne il libero esercizio; o per limitare la libertà di parola, o di stampa; o del diritto del popolo di riunirsi pacificamente, e di sottoporre al Governo petizioni affinché si ponga rimedio ai reclami".

Il 26 giugno 1997, trovando gli argomenti del Governo "straordinariamente non persuasivi", la Corte dichiarava la parziale incostituzionalità della legge, tenuto conto della "particolare natura del mezzo", e cioè di internet. Innanzi ai vincoli che, in nome della libertà d'espressione, sono posti alla volontà del legislatore, quest'ultimo avrebbe dovuto dimostrare la fondatezza e proporzionalità delle misure adottate. Ma, con le parole del giudice estensore, *justice* Stevens: "La drammatica espansione di questo nuovo mercato delle idee contraddice le basi fattuali dell'argomento del Governo. I dati dimostrano che la crescita d'internet è stata e continua ad essere fenomenale. Secondo la tradizione costituzionale [di questo paese], mancando evi-

denza in senso contrario, presumiamo che sia più probabile che la regolamentazione da parte del governo circa il contenuto dei messaggi ostacoli il libero scambio delle idee, piuttosto che incoraggiarlo".

D'altra parte, passando al secondo caso da prendere in esame, si tratta della lite C-101/01, nota anche come caso *Lindqvist*, deciso dalla Corte di giustizia di Lussemburgo il 6 novembre 2003. La questione interessa il secondo degli scenari prima evidenziati, vale a dire i casi in cui il legislatore è intervenuto con una normativa che, nondimeno, lascia taluni problemi fondamentali, aperti a soluzioni anche opposte.

In particolare, la causa aveva avuto origine con il procedimento penale intentato dalle autorità svedesi contro la signora Lindqvist, alla fine degli anni novanta, allorché l'imputata, nel corso delle attività lavorative come catechista presso la parrocchia di Alseda, aveva creato una pagina web in cui riportava notizie e aneddoti riguardanti se stessa e altri diciotto parrocchiani, alcuni di questi indicati con nome, cognome e numero di telefono, descrivendone altresì mansioni e hobby, sebbene, come ammette la Corte, in forma spesso carina e non priva di humour. Uno dei problemi emersi con l'uso dei personal computer e la creazione delle prime pagine web personalizzate era infatti se le informazioni immesse in questo modo su internet, dovevano ritenersi trasmesse anche a paesi non appartenenti all'Unione europea. La ragione del problema dipendeva dal fatto che la prima normativa comunitaria in materia di tutela e protezione dei dati personali, ossia la direttiva 46 del 1995 (D-95/46/CE) stabiliva – e tuttora distingue tra – un regime generale che fissa le condizioni di legittimità del trattamento dei dati personali all'interno dell'Unione, e un regime speciale, con regole specifiche, per consentire agli Stati membri di monitorare il trasferimento di quei dati ai paesi terzi. In quest'ultima ipotesi, ai sensi dell'art. 25 della direttiva, non soltanto il trasferimento può aver luogo a condizione che il paese terzo garantisca un "livello di protezione adeguato"; ma, al fine di esprimere un giudizio sul livello di adeguatezza, sono previste, altresì, procedure di consultazione tra la Commissione europea e gli stati membri.

Tuttavia, come notava la Corte di giustizia nel caso *Lindqvist*, bisogna pure ammettere che "la direttiva 95/46 non definisce l'espressione trasferimento a un paese terzo nell'articolo 25 o in ogni altra disposizione" (*op. cit.*, § 56 della decisione). In altre parole, il legislatore comunitario del 1995 non aveva saputo anticipare gli scenari di ciò che di lì a poco, e in retrospettiva, sarebbe stato chiamato il Web 2.0. Da un lato, caricando i propri (e altrui) dati sulle pagine del web, secondo ciò che ancora oggi avviene evidentemente su Facebook o Google+, è innegabile che questi ultimi dati siano potenzialmente messi a disposizione di chiunque nella rete. Ma, d'altro canto, se dovessimo intendere ciò come un trasferimento dei dati anche a paesi terzi, varrebbe di conseguenza il regime speciale previsto dall'art. 25 della direttiva, per cui le regole specifiche del monitoraggio previsto per il trasferimento dei dati avrebbero comportato l'appesantimento, per non dire lo strangolamento, del flusso di informazioni immesse in Europa sul web al resto del pianeta. Per far fronte al dilemma e, con questo, alla lacuna che si era venuta a creare per via dell'innovazione tecnologica, la Corte di giustizia europea prendeva un'encomiabile decisione politica, facendo ricorso al buon senso: "non c'è trasferimento [di dati] a paesi terzi ai sensi dell'art. 25 della direttiva 95/46, quando una persona fisica dello stato

membro immetta dati personali su una pagina internet che è stata ospitata dal proprio fornitore di servizi, con sede in quello stato o in un altro stato membro, per ciò stesso rendendo accessibili quei dati a chiunque si connetta a internet, ivi incluse persone di uno stato terzo" (§ 71 della sentenza).

Eppure, ed è questo il punto sul quale preme ora attirare l'attenzione, potremmo proseguire il nostro elenco di leggi e sentenze che hanno avuto per oggetto la disciplina giuridica d'internet nel corso degli ultimi decenni, senza per questo esaurirne i problemi e le sfide. La complessità del fenomeno che s'intende regolare travalica infatti, più spesso, la tradizionale dialettica tra gubernaculum e iurisdictio, consigliando d'indagare piuttosto il più vasto e intricato reticolo di attori e organi istituzionali, entro il quale, in realtà, quella dialettica va in definitiva collocata. Nel compendiare, ancora una volta, il passaggio dalle tradizionali forme di governo a quelle della governance con la parola "complessità", vediamo dunque nel prossimo paragrafo i nuovi termini, secondo cui la questione va affrontata.

### 3.4.2. *La complessità di internet*

Dei tre significati della complessità giuridica, illustrati con la figura 5 del capitolo secondo, vale la pena di soffermarci qui sul primo di essi, cioè a dire la complessità intesa nel senso della maggiore o minore comprimibilità algoritmica delle informazioni. Per comprendere perché la tradizionale dialettica tra gubernaculum e iurisdictio non riesca a dar del tutto conto della complessità del fenomeno indagato, bisogna infatti muovere dalla struttura e funzionamento d'internet, per cui, a ben vedere, esaminandone la disciplina giuridica, occorre distinguere quanto meno tre (Benkler 2007), se non quattro (Cerf e al. 2013), livelli o piani d'analisi:

i) il livello fisico delle infrastrutture che consentono di accedere alla rete e ne garantiscono la connettività;
ii) il livello logico della rete che rende possibile il flusso dei dati e informazioni tramite il dominio dei nomi e indirizzi, protocolli e altri standard;
iii) il livello dei contenuti attinente alla produzione e scambio tra gli utenti delle risorse in rete. Rispetto alla tripartizione di Benkler (v. Durante 2007: 1-2), è a questo livello che il "capo evangelista d'internet per Google", Vinton Cerf, propone un'ulteriore distinzione, ossia:
iv) il livello dei contenuti soggetti alle diverse discipline giuridiche in tema di reati informatici, diritto d'autore, protezione dati, ecc., distinto dal livello sociale inerente alla tutela dei diritti umani, la fiducia in rete, l'identità digitale, e così via (Cerf e al. 2013: 7).

Questa distinzione è cruciale perché, a seconda del livello indagato, non soltanto muta il ruolo degli stati nazionali e delle organizzazioni internazionali, ma cambia anche il novero delle ulteriori istituzioni, enti e società, coinvolti. Così, se prestiamo attenzione al livello logico e delle infrastrutture (livelli i-ii), avremo a che fare con certe agenzie internazionali come l'ITU, acronimo inglese per l'Unione internazionale delle telecomunicazioni, ma non con altre, come il WIPO, o Organizzazione mondiale per la proprietà intellettuale, il cui ruolo, invece, è rilevante a livello sociale e di contenuti (livelli iii-iv).

Stesso discorso vale per gli enti, organizzazioni e società che contribuiscono al funzionamento della rete, soprattutto sul versante logico (ii), e secondo una ben specifica divisione dei compiti. Senza fini di completezza, ma a solo scopo illustrativo, abbiamo:

a) l'*Internet Engineering Task Force* (IETF), organizzazione non governativa, alla quale si partecipa a titolo personale, e che si occupa dello sviluppo e promozione dei protocolli e standard di internet, in collaborazione con il *Consorzio per il World Wide Web*, o W3C, il cui odierno presidente è proprio il "padre del Web", Tim Berners-Lee (n. 1955);

b) la *Società Internet* (ISOC), organizzazione internazionale non-profit con base giuridica statunitense, fondata dai pionieri d'internet nel 1992, i cui soci sono sia singoli individui che aziende, sia organizzazioni che governi e università, e il cui scopo statutario è di "promuovere lo sviluppo aperto, l'evoluzione e l'uso di internet per il bene della popolazione di tutto il mondo";

c) il *Consiglio per l'Architettura d'Internet* o *Internet Architecture Board* (IAB), che svolge sia funzioni di sorveglianza sull'IEFT (v. sopra (a)), sia di consulenza per l'ISOC (v. sopra (b));

d) l'*ICANN*, acronimo inglese per *Internet Corporation for Assigned Names and Numbers*, formalmente società di diritto privato con sede in California che, dal 1998, subentrando all'agenzia statunitense IANA, ha, tra i vari compiti, quello di assegnare gli indirizzi in rete (IP), e gestire il sistema dei nomi a dominio di primo livello[2], nonché il codice internazionale (".it", per l'Italia).

Oltre agli organismi internazionali e alle organizzazioni non governative con mansioni tecniche, dovremmo poi aggiungere le comunità di gruppi d'esperti che, a vario titolo, si occupano anch'esse della rete, come nel caso dell'*Istituto degli ingegneri elettrici ed elettronici* (IEEE) con sede a New York, l'*Iniziativa per la rete globale* o *Global Network Initiative* (GNI), organizzazione non governativa il cui scopo è di tutelare la privacy degli individui e ostacolare la censura in rete da parte degli stati autoritari, il *Comitato mondiale per la libera stampa* o *World Press Freedom Committee* (WPFC), il cui scopo è invece la difesa e sviluppo della stampa libera, ecc.

Infine, un riferimento va all'*Internet Governance Forum* (IGF), i cui incontri annuali, sotto gli auspici delle Nazioni Unite, hanno avuto inizio nel 2006 e che rappresenta, in qualche modo, una sorta di assemblea partecipativa democratica in cui tutte le varie componenti del mondo della rete sono chiamate a dialogare e misurarsi.

Rispetto a questo intricato reticolo di attori, pubblici e privati, sono stati proposti diversi tipi di governance, riassumibili, in sostanza, secondo cinque modelli (Solum 2009: 56-57):

i) il modello degli ordini spontanei che, sulla scia di Hayek, abbiamo introdotto nel capitolo secondo (§ 2.2);

ii) il modello delle istituzioni transnazionali e delle organizzazioni internazionali fondate sugli accordi degli stati;

---

[2] Si tratta degli esempi ben noti relativi agli indirizzi internet che terminano con ".com", ".org", ".edu", e via dicendo.

iii) il modello tecnologico imperniato sull'architettura della rete e sul fatto che molte delle decisioni riguardano i protocolli d'internet e altri standard logici, che ne determinano il funzionamento;

iv) il modello statale che fa leva sul ruolo crescente della legge per fronteggiare i problemi che derivano dallo stesso sviluppo d'internet;

v) il modello economico per cui molte delle decisioni fondamentali inerenti alla rete, in realtà, dipendono dal gioco delle forze del mercato.

Lasciando per ora in sospeso il modello cui si ispirano i regimi autoritari, ossia, va da sé, il quarto, è ragionevole sostenere che, nei sistemi costituzionali d'occidente che si ispirano viceversa alla tradizione liberal-democratica (§ 3.2.1), si verifichino degli "ibridi che incorporano alcuni elementi di tutti i cinque modelli" (Solum 2009: 87).

Ma, tornando alla questione dalla quale eravamo partiti, come possiamo intendere e posizionare il tradizionale intervento giuridico degli stati, tra gubernaculum e iurisdictio, all'interno del complesso insieme dei meccanismi regolatori della rete?

Sulla scorta della quadripartizione di Cerf et al. (2013), la risposta non può che essere differenziata, e riassumibile a grandi linee sulla base di uno spettro in cui, ad un estremo, il modello statale svolge un ruolo di primaria importanza al livello dei contenuti della rete. Questo ruolo, poi, si attenua man mano al livello fisico delle infrastrutture, dove l'intervento degli stati si disloca sul piano del diritto internazionale tradizionale, tramite organismi come l'ITU e nella contrattazione con le imprese multinazionali, nonché a livello sociale, dove gli interventi degli organismi nazionali e internazionali si intrecciano con le linee guida e azioni di organizzazioni non governative. All'estremo opposto dello spettro, invece, il ruolo degli stati è marginale al livello logico d'internet, salvo la pressione indiretta che qualche stato, come gli Stati Uniti, può ancora esercitare sulle decisioni di alcuni organismi come l'ICANN. A conferma dell'assunto, basti pensare come la Cina, che pur controlla il livello fisico delle infrastrutture tramite le imprese di stato, debba poi isolare la propria rete dal resto del mondo con ciò che viene comunemente compendiato come la "grande muraglia di fuoco". Attraverso il sistematico filtraggio dei contenuti immessi in rete, il fine è quello di neutralizzare il livello logico d'internet che è, appunto, sottratto all'autorità di quel paese.

Nel passaggio dalle forme tradizionali d'intervento degli stati agli odierni assetti della governance, vediamo come quest'ultima irrilevanza del modello statale al livello logico della rete si concreti con un esempio.

### 3.4.2.1. *L'esempio di ICANN*

Si è già introdotta in precedenza la figura d'ICANN e il fatto che le sue decisioni determinino l'intera infrastruttura del sistema, garantendo un unico dominio di nomi e numerazione per internet, con un approccio "dall'alto verso il basso" che si avvale, però, della collaborazione di un sistema di registri regionali. Qui, il ruolo degli stati è limitato a una mera funzione consultiva, sebbene molte delle decisioni possano avere alta incidenza politica, economica e sociale. Ai sensi dell'articolo XI, sezione 2.1 dello statuto, come emendato l'11 aprile 2013, il Comitato consultivo dei Governi può semplicemente "presentare istanze al Consiglio in via diretta, ora sotto forma di commento ora di parere preventivo, oppure raccomandando una

specifica azione o una nuova politica di sviluppo o la revisione degli indirizzi assunti". Nei confronti delle decisioni dell'ICANN su come assegnare gli indirizzi in rete, gestire il sistema dei nomi a dominio di primo livello o il codice internazionale, gli stati sovrani, in altri termini, non dispongono di alcun potere di veto.

Questa situazione di fatto e di diritto, va da sé, ha attirato le critiche di molti, specie se si considera la struttura a dir poco bizantina di un organismo, come quello di ICANN, senza nessuna particolare legittimazione democratica e che, nondimeno, prende decisioni delicate come, ad esempio, se introdurre nuovi nomi a dominio come ".gay" o ".sex", o a denominazione geografica controllata come ".patagonia". Sebbene, in accordo con la migliore tradizione dualistica dell'ordinamento, ICANN preveda fin dalla sua istituzione le modalità per la risoluzione imparziale delle controversie – attualmente note come *Uniform Dispute Resolution Policy* (UDRP) – non sorprenderà che ci siano stati tentativi per modificare l'odierno stato dell'arte. Alla dodicesima conferenza mondiale sulle telecomunicazioni internazionali, o *World Conference on International Telecommunications* (WCIT-12), nel dicembre 2012, molti governi nazionali hanno rivendicato il loro diritto a gestire in prima persona le sorti d'internet, sia sul piano logico sia infrastrutturale, con particolare riguardo al sistema dell'assegnazione, distribuzione e reclamo nel settore dei nomi a dominio. In sostanza, la proposta dei governi è stata di sottrarre questo ambito all'autorità di ICANN, per affidarlo a una già nota agenzia internazionale, l'ITU, sotto il controllo degli stati sovrani.

Tuttavia, quello che può sorprendere del dibattito al WCIT-12 svoltosi a Dubai, è la provenienza dell'attacco: i critici delle competenze tecnocratiche d'ICANN non sono certo stati i rappresentanti degli stati democratici occidentali ma, significativamente, certi campioni dei diritti umani come la Cina, la Russia, l'Arabia Saudita, gli Emirati Arabi, l'Algeria, il Sudan e l'Egitto. In appoggio all'ICANN e di qui, paradossalmente, a favore della perdita delle proprie competenze normative in questo cruciale settore d'internet, si sono schierati gli Stati Uniti, l'Unione europea, il Canada e pochi altri paesi.

### 3.4.3. *Criteri normativi*

Non mancano dunque i problemi d'internet con la sua governance: nonostante la rete abbia fin qui palesato una straordinaria capacità d'auto-organizzazione, generando a getto continuo nuove forme d'ordine spontaneo, rimangono tuttavia aperte tutta una serie di questioni. Ancora una volta senza pretese di esaustività, è sufficiente segnalare il dibattito sull'opportunità di una nuova generazione di diritti, tra cui un diritto universale d'accesso a internet, e come tutelare "vecchi" diritti come la protezione della privacy e dei dati personali, i diritti di proprietà intellettuale e via discorrendo. A ciò si aggiunga l'accesa discussione ancora in corso sulla neutralità della rete e, cioè, se e in che misura i grandi connettori di internet, ossia le multinazionali delle telecomunicazioni, possano legittimamente discriminarne i contenuti, differenziando i servizi a seconda del sito, utente, piattaforma o applicazione, come nel caso dei servizi web o in peer-to-peer. Inoltre, rimane ancora in sospeso il ruolo da assegnare agli stati, anche per il tramite di organizzazioni internazionali come le Nazioni Unite, specialmente ai livelli logico e dei contenuti.

Come già segnalato (§ 3.1.3.1), tale insieme di non facili decisioni appare del resto aggravato dal fatto che non disponiamo, allo stato, di una teoria alla quale affidarci e con cui prendere posizione rispetto ai fenomeni in corso. Davanti al plesso di criteri e principi elaborati dalla tradizione giuridica e politica, basterebbe rimarcare come la rivoluzione tecnologica incida su uno dei suoi presupposti cardinali, vale a dire il pilastro della territorialità sul quale gli ordinamenti sono venuti basandosi da secoli. Il fatto che gli ordinamenti su internet siano viceversa posizionati, per definizione, su uno spazio virtuale, rende a dir poco problematica la trasposizione meccanica dei consueti concetti di democrazia, rappresentanza, contratto sociale o giurisdizione. Da un lato, come riferito in precedenza (§ 1.4.3), il tradizionale intervento degli stati, imperniato sulla minaccia di sanzioni fisiche, risulta spesso inefficace in questo nuovo contesto, quand'anche fosse solo limitato al livello dei contenuti d'internet. D'altro canto, nel tentativo di disciplinare gli effetti extraterritoriali dell'interazione sociale sulla rete, gli stati corrono il rischio di violare un altro principio cardine dello stato di diritto, cioè a dire, con Rousseau (§ 3.1.2), quello di (tentare di) imporre leggi su individui che non hanno avuto alcun modo di prendere parte, sia pure mediante processi di democrazia indiretta o rappresentativa, a quelle stesse decisioni.

Approdiamo su queste basi a un paradosso che, in realtà, riporta ai dilemmi tra globalisti e realisti (§ 3.3.2). Come già suggerivano questi ultimi nel campo del diritto internazionale, la governance di internet sta in sostanza a segnalare, con buona pace dei globalisti, il modo in cui dalla complessità sociale emergano forme spontanee d'ordine che, nel trascendere la volontà programmatrice dei legislatori, hanno fin qui garantito quanto la Corte suprema americana definiva come "la drammatica espansione di questo nuovo mercato delle idee" (v. § 3.4.1). Eppure, la pletora dei problemi che rimangono in attesa di risposta – dalla neutralità della rete al ruolo degli stati – ricorda, al modo dei globalisti, che occorre un insieme di criteri normativi con cui intendere le nuove forme del rapporto tra rappresentanza politica e decisioni giuridiche, al fine di stabilire ciò che si può o non si deve fare nella governance d'internet. Sostenere, come fa Solum (2009: 87), che quest'ultima non possa che essere un ibrido dei vari modelli d'ordine spontaneo, su scala transnazionale o internazionale, in chiave tecnologica, statale o economica, non è sufficiente. Nel passaggio dalle vecchie forme di governo a quelle della governance, e in attesa di un nuovo Locke che stili i nuovi *Due trattati sulla governance* (v. § 3.1.1), come orientarsi?

Astrattamente, al modo dei globalisti, i giuristi dispongono sia di criteri sostanziali sia formali, per far fronte alle sfide della governance odierna. Quanto ai criteri sostanziali, è il caso di richiamarsi ai principi di giustizia della tradizione liberale risalente a Locke e alle successive dichiarazioni dei diritti dell'uomo (§ 3.1.3). Quanto ai criteri formali, basti pensare alla nozione di terzietà del contrattualismo come garanzia di equidistanza e imparzialità di giudizio, cui vanno ad aggiungersi ulteriori parametri, quali la natura pubblica e intellegibile del diritto come informazione nel senso di Hobbes (§ 2.1.2.1). Per non smarrire la dinamica degli ordini spontanei messa in risalto dai realisti, conviene tuttavia integrare i parametri sostanziali e formali dell'analisi in chiave processuale. Seguendo in questo la saggezza dei giuristi romani, il primo passo spetta infatti a chi afferma e non, certo, a chi nega le ragioni del contendere: *onus probandi incumbit ei qui dicit, non ei qui negat*.

Su queste basi, possiamo far tesoro degli elementi fin qui acquisiti nel corso dell'indagine e affrontare i problemi della governance in tre fasi, ossia concependo il rapporto tra rappresentanza politica e decisioni giuridiche nei termini di a chi spetti l'onere della prova, con il dovere di conoscenza e la scelta degli strumenti giuridici richiesti dai problemi che si ha innanzi. Gli ultimi paragrafi del presente capitolo saranno dedicati rispettivamente a ciascuno dei tre criteri ora proposti.

#### 3.4.3.1. *L'onere della prova*

Il primo criterio da cui partire per giungere a un appropriato bilanciamento tra rappresentanza politica e decisioni giuridiche, consiglia di prestare attenzione alle forme d'ordine spontaneo nella rete. Ciò significa che l'onere della prova ricade su coloro i quali intendono governare questi processi, secondo la dialettica hayekiana di *kosmos* e *taxis* (v. § 2.2.1). In sostanza, è onere di quest'ultima, sia sul fronte tradizionale del governo, sia su quello odierno degli attori della governance, argomentare la carenza auto-organizzatrice del *kosmos* e, quindi, la necessità stessa dell'intervento.

Questo meccanismo, del resto, non è nuovo né richiede una dimensione digitale. Al contrario, lo abbiamo già visto in due occasioni:

i) nel § 3.3, a proposito del principio di sussidiarietà, si è riferito che spetta all'ente, per così dire, posizionato su scala maggiore, l'onere di mostrare che gli obiettivi dell'azione proposta non possono essere conseguiti in maniera sufficiente dall'ente collocato su scala minore: l'Unione europea nei confronti dei suoi stati membri, lo stato nazionale nei confronti degli enti regionali o locali, ecc.

ii) nel § 3.4.1, a proposito della decisione presa dalla Corte suprema statunitense sulla legittimità di alcune disposizioni del *Communications Decency Act*, si è visto, analogamente, che era il governo a dover dimostrare come le regolamentazioni proposte servissero a incoraggiare, piuttosto che a ostacolare, il libero scambio delle idee.

Questo meccanismo sembra ancor più utile nel caso dell'odierna governance, stante la pletora di attori, enti, organismi e organizzazioni che, ai vari livelli nazionali, internazionale o transnazionale, possono potenzialmente prendere delle decisioni. Al tempo stesso, il criterio non mira a difendere semplicemente lo status quo, congelando per così dire il presente, né intende offrire una visione salvifica del *kosmos*, dato che è, appunto, sempre possibile intervenirvi, una volta mostrata la necessità dell'ingerenza.

#### 3.4.3.2. *Il dovere di conoscenza*

Il secondo criterio proposto è una conseguenza del primo: al fine di mostrare la necessità dell'intervento della *taxis*, sia sul piano del governo, sia da parte degli attori della governance, questi ultimi devono pur conoscere la materia che s'intende disciplinare. Al lettore (o studente) l'affermazione può sembrare un'ovvietà: eppure, gli esempi contrari purtroppo abbondano. Per rimanere ai casi già visti, basti tornare al WCIT-12 (§ 3.4.2.1), allorché, nel dibattito che condusse alla conferenza di Dubai, si discuteva su un nuovo modello economico con la proposta dell'Associa-

zione degli operatori europei per la rete di telecomunicazioni (ETNO, secondo l'acronimo inglese); vale a dire il gruppo dei fornitori europei di tali servizi che comprendono, tra gli altri, Telecom Italia, Telefónica de España, France Telecom e la Deutsche Telekom. Senza entrare nei dettagli tecnici della proposta, basti dire che la decisione della presidenza WCIT-12 fu di spostare il dibattito nella sede di un altro organismo a noi noto, ossia l'ITU (§ 3.4.2); e, più in particolar modo, di affidare il progetto alle cure della divisione dell'Unione internazionale delle telecomunicazioni che si occupa degli standard per il design: ITU-T. "Per analogia, sarebbe come dire che qualcuno porti i propri problemi relativi alle tasse a un architetto, piuttosto che a un ragioniere abilitato o a qualche altro esperto in tasse. Certamente, un architetto è educato, iscritto all'albo e può finanche avere la sua opinione personale sulle tasse e il denaro – e perfino su come certe tecniche di costruzione possano essere meno care o comportare una riduzione delle tasse. Nondimeno, per dire un'ovvietà: gli architetti costruiscono e disegnano case, mentre un ragioniere abilitato ha a che fare con tasse e denaro" (Cerf e al. 2013: 17-18).

Nel caso di specie, si può avanzare il dubbio che la presidenza WCIT-12 fosse pienamente a conoscenza che gli esperti della divisione ITU-T per gli standard sul design delle telecomunicazioni non sono anche esperti dei nuovi modelli economici per internet: piuttosto, la decisione andrebbe interpretata come uno stratagemma per spostare alcune scelte critiche sul futuro d'internet nell'ambito di organi internazionali sotto il controllo o direzione degli stati. Ma anche se così fosse, in questo come in altri casi, l'astuzia, o la malafede delle scelte, cadrebbe sotto la scure del secondo criterio normativo qui proposto. Infatti, bisogna pur ricorrere all'ipotesi che coloro i quali avanzano un intervento della *taxis* infondato, in realtà non ne conoscano l'oggetto, proprio per evitare che l'infondatezza delle loro scelte sia tacciata come semplice astuzia, o atto di malafede. E però, se non ne conoscono l'oggetto, cade anche la possibilità di averne mostrato la necessità dell'intervento. Soltanto a patto di conoscere la materia, potrà in fondo discutersi della scelta degli strumenti.

### 3.4.3.3. *La scelta degli strumenti*

Il terzo e ultimo criterio consegue dai due precedenti: una volta argomentata la necessità dell'intervento, perché se ne conosce l'oggetto, segue l'esigenza di stabilirne sia il livello, sia le modalità, secondo ciò che abbiamo avuto modo di illustrare con la figura 3 del § 1.1.3, a proposito del diritto come meta-tecnologia.

Sul piano dei contenuti, tornano alla ribalta i parametri sostanziali cui si è fatto prima cenno (§ 3.4.3), sia per quanto attiene ai criteri di giustizia, sia ai principi fondamentali e alle norme vigenti negli svariati settori dell'ordinamento; sebbene, proprio per questo, si ripresenti a questo punto la necessità di precisare il piano e tipo d'intervento normativo richiesto.

Per quanto concerne il livello d'intervento, esso può essere ora internazionale, ora nazionale e, in quest'ultimo caso, essere ulteriormente distinguibile in regionale, provinciale, comunale, ecc.

Invece, per quanto riguarda le modalità d'intervento, queste ultime possono consistere nei tipici strumenti di disciplina coattiva come la legge, oppure tradursi nei mezzi della disciplina autoritativa, più spesso indicata come *soft law*, come nel caso di codici di condotta e auto-regolamentazione, raccomandazioni, opinioni, ecc.

In entrambi i casi, si tratta di specificare il ruolo della governance secondo temi e motivi che finiscono per intrecciarsi con quelli di un altro settore, al quale gli studiosi dedicano per lo più un capitolo a sé stante nelle proprie trattazioni sugli ordinamenti giuridici, vale a dire le fonti del diritto. Lo studio della dinamica dei processi istituzionali va per ciò integrato con l'esame della statica del sistema: nel prossimo capitolo, avremo occasione d'indagare livelli e modalità d'intervento del sistema giuridico, formalizzando quali siano le fonti del XXI secolo. Su queste basi, sarà poi possibile tornare a misurarsi con la sostanza dei problemi giuridici con cui sono oggi alle prese le società ICT-dipendenti.

# IV.
# *Fonti*

> "L'autorità delle leggi che poggiano esclusivamente sul consenso, dipende interamente dall'autorità politica, ed è legge sempre valida questa: nessuna legge civile è eterna"
>
> Francis BACON

Nel corso dei capitoli precedenti si è fatto riferimento allo studio delle fonti del diritto, come esame della "statica del sistema", in opposizione alla dinamica rappresentata dall'analisi del passaggio dalle tradizionali forme di governo all'odierna governance. Del resto, l'affermazione si giustifica, avendo presente il significato letterale del termine fonte, ossia il luogo dal quale una sorgente d'acqua ha origine o dove l'acqua stessa scaturisce. Per questo verso, come attestano i manuali universitari in campo giuridico, la metafora designa innanzitutto ciò che non muta, o non dovrebbe mutare, nel perenne fluire della prassi: la statica, appunto, del sistema.

Come tutte le metafore, tuttavia, anche questa delle fonti va presa, come suol dirsi, con un grano di sale (anzi due). In primo luogo, è da tener presente che fin dall'inizio della sua formulazione, con la generazione dei grandi giuristi romani che fa capo a Cicerone (106-43 a.C.), il significato della metafora delle fonti ha dato il via a innumerevoli interpretazioni. Mentre, nel caso di Cicerone, essa esprime classicamente la visione giusnaturalistica del diritto[1], già con la generazione successiva, alla fine del primo secolo a.C., la metafora della fonte viene ripresa da Tito Livio (59 a.C.-17 d.C.), nel libro terzo delle *Storie*, per riferirla non solo all'"essenza della natura" ma alla Legge delle XII Tavole[2]. Ripresa dai glossatori nel Medioevo e dai giusnaturalisti moderni, l'immagine è stata sfruttata del pari dai cultori del giuspositivismo, salvo poi essere declinata, ora, al modo dell'illustre giurista tedesco Friedrich Carl von Savigny (1779-1861), come "spirito del popolo", ora, al modo del

---

[1] Si v. *Delle Leggi*, I, 16-18: "Se questo ragionamento è esatto, e certo a me per lo più sembra tale, la fonte del diritto è da ricavare dalla legge; essa è infatti l'essenza della natura, essa è mente e ragione del saggio, essa criterio del giusto e dell'ingiusto" (Cicerone ed. 1974: 429).

[2] Si v. *Storie*, III, 34, 6: "Le leggi delle dieci tavole furono approvate nei comizi centuriati: esse ancor oggi, in questo immenso cumulo di leggi sovrappostesi le une dopo le altre, sono la fonte di tutto il diritto pubblico e privato. Si diffuse poi la voce che mancassero ancora due tavole …" (Livio ed. 1979: 527). Questa tradizione giungerà fino al Digesto (1,2,2,6), dove rimane in parte custodita per il tramite di Pomponio.

giurista italiano Santi Romano (1875-1947), in rapporto alla nozione di "necessità". Di fronte a questi, e altri possibili, significati della metafora, non sorprende che un altro giurista a noi già noto, Hans Kelsen, fin dalla prima edizione della *Dottrina pura del diritto* (1934), dichiarasse che "l'ambiguità del termine 'fonte del diritto' fa sì che non lo si possa in nessun modo utilizzare" [3].

Il secondo grano di sale con cui prendere la metafora delle fonti come statica del sistema, è offerto dalla tesi del Lord Cancelliere inglese Francis Bacon (1561-1626), che non a caso serve da epigrafe per il presente capitolo. La stabilità trasmessa dall'immagine della fonte, come luogo dal quale sgorga il diritto, va infatti intesa relativamente e, cioè, in rapporto alle trasformazioni che occorrono, sul piano dei fattori di produzione normativa dell'ordinamento, in tutti i sistemi giuridici. Valga, per ora, l'esempio dell'ICANN, su cui sopra § 3.4.2.1, che illustra come, in un settore chiave degli odierni sistemi giuridici, il ruolo degli stati si sia ridotto a una mera funzione consultiva, per cui decisioni ad alta incidenza politica, economica e sociale, sono prese da una società di diritto privato con sede in California. Il fatto che i governi e gli stati nazionali, vecchi monopolisti delle fonti del diritto, abbiano anche di recente tentato di privare ICANN dei suoi poteri decisionali, sta a segnalare come le diverse interpretazioni della metafora non siano innocue ma, in realtà, le trasformazioni che occorrono sul piano delle fonti siano legate a questioni di potere.

Sulla base di queste premesse, possiamo trarre due prime conclusioni. La prima è che, in nome delle fonti, i giuristi mirano a formalizzare e, dunque, a tener per fermo le modalità attraverso le quali il diritto sorge, muta e si estingue in un dato contesto storico e sociale. Questa formalizzazione, in secondo luogo, non significa che tali modalità non cambino ma, piuttosto, che le forme di questo cambiamento si strutturano secondo processi di lunga durata, che gli storici compendiano tramite l'ulteriore stilizzazione di modelli: il sistema antico e medioevale delle fonti del diritto, il paradigma di Westfalia e l'odierno stato dell'arte. Dal punto di vista estetico, questa è la ragione per cui, al posto delle figure con cui abbiamo presentato gli osservabili dell'analisi nelle pagine precedenti, il presente capitolo si avvarrà invece di schemi o tabelle per illustrare i diversi modelli delle fonti.

Più in particolare, il presente capitolo si snoda lungo tre punti principali. A continuazione (§ 4.1), muoveremo dalla definizione standard di fonte che, nonostante le dichiarazioni della *Dottrina pura del diritto*, deve essere ricondotta al pensiero di Kelsen; sia pure, come diremo, a due condizioni. Bisogna infatti integrare la definizione standard con le cosiddette fonti *extra* e *contra ordinem* dell'ordinamento (§ 4.1.1); e, in omaggio alla visione dualistica del diritto, in rapporto alla giurisprudenza come fonte (§ 4.1.2).

Il secondo osservabile dell'analisi viene compendiato come modello di Westfalia, nel ricordo del trattato che pose termine alla guerra dei trent'anni (1648) e che, per secoli, ha rappresentato il punto di riferimento per il modello delle fonti invalso tra i moderni (§ 4.2). La ragione dell'approccio è triplice: esso consente di chiarire cos'è

---

[3] Kelsen ed. 1952: 83. Non senza una buona dose d'ironia, come vedremo sotto § 4.1, è proprio a Kelsen che dobbiamo la straordinaria fortuna di cui la metafora della fonte ha continuato a godere lungo tutto la seconda metà del secolo scorso, fino a oggi.

mutato rispetto al precedente modello medioevale delle fonti (§ 4.2.1); perché il modello di Westfalia può essere convenientemente riassunto in chiave "monista" (§ 4.2.2); per giungere ai motivi della sua crisi (§ 4.2.3).

La parte finale del capitolo riguarda l'attuale assetto delle fonti, presentato come fonti delle società ICT-dipendenti (§ 4.3). Le variabili del terzo osservabile dell'analisi sono date dai mutamenti occorsi sul piano del diritto nazionale (§ 4.3.1), del diritto internazionale (§ 4.3.2), e con le nuove frontiere del diritto transnazionale (§ 4.3.3). Alla luce dell'odierno quadro delle fonti, saremo in grado di cogliere un ulteriore aspetto che connota l'impatto della rivoluzione tecnologica sul diritto, vale a dire il ruolo del design sul piano delle fonti e delle istituzioni, che sarà l'oggetto del capitolo quinto.

## 4.1. *Il legato di Kelsen*

È a Kelsen che dobbiamo l'odierna definizione standard di fonte che gli studiosi, nonostante il dissidio filosofico sull'informazione giuridica come realtà (v. sopra figura 7 in § 2.1.2.2), hanno adottato.

In buona sostanza, i giuristi intendono per fonti del diritto le "meta-norme di produzione normativa dell'ordinamento", vale a dire le norme che disciplinano le forme attraverso cui si crea, si modifica o si estingue il diritto in un dato sistema giuridico. Per dirla con le parole di un esimio giurista ricordato in precedenza (§ 2.3.1), "le fonti vengono oramai considerate, larghissimamente, quali fattori giuridici dell'ordinamento, previsti e disciplinati da apposite norme costitutive dell'ordinamento stesso" (Paladin 1996: 17).

Per rendere ora più concreta la definizione e, con questa, il legato di Kelsen, si prenda in considerazione l'esempio di un esame universitario o la multa comminata da un vigile urbano. Si tratta di atti che possono qualificarsi come giuridicamente rilevanti solo a due condizioni:

i) l'atto, che è poi una norma, deve essere posto da chi ne ha la competenza: l'esame che lo studente darà, magari sulla scorta di questo libro, sarà valido se, e solo se, il professore che vi farà l'esame ne ha il titolo sulla base dell'incarico ricevuto dal proprio dipartimento e, in certi casi, sulla base di un decreto rettorale. A sua volta, nel caso della multa, questa sarà valida se, e solo se, la persona fisica che vi contesterà una data infrazione ne avrà titolo, sulla base dell'atto con cui è stata nominata vigile urbano. Ciò spiega perché chi scrive questo libro, e farà magari l'esame universitario a qualche lettore, non abbia titolo per contestarvi il fatto che, per sostenere l'esame, avete abbandonato la macchina in divieto di parcheggio. Viceversa, il vigile urbano, che starà intanto lasciando il verbale della multa appiccicato sul parabrezza della vostra macchina, non potrebbe tuttavia interrogarvi ai fini dell'esame universitario; e ciò, poniamo, nonostante il vigile sia un brillante cultore di filosofia del diritto!

ii) quella norma particolare, che è poi l'esame universitario o la multa del vigile, sarà d'altro canto valida, solo in ragione di un'ulteriore norma sovraordinata che la dota, appunto, di validità: le norme del codice della strada nel caso della multa del

vigile; oppure, nel caso dell'esame di cui sopra, le norme in materia di organizzazione dell'università. Dal piano amministrativo, si passa di qui, necessariamente, al livello gerarchicamente sovraordinato definito dalla legge come fonte del diritto. La legge è infatti fonte perché, nei nostri esempi, è la norma che fissa i modi in cui altre norme, ad essa sottordinate, possono creare, modificare o estinguere il diritto in un ordinamento dato.

Questa doppia condizione, nondimeno, solleva due problemi: l'uno risolto in modo brillante da Hobbes, l'altro destinato ad essere la croce di Kelsen.

Nel primo caso, si tratta del problema della consuetudine, vale a dire di quel fatto normativo che abbiamo incontrato sopra, a proposito delle forme dell'emergenza (§ 2.2). Assunto a modello il giuspositivismo di Hobbes (§§ 2.1.2.1 e 3.1.1), per cui è soltanto la volontà del sovrano che può assurgere a fonte del diritto, come poteva egli dar conto del sistema del proprio paese, l'Inghilterra, a schietta base consuetudinaria?

Con qualche secolo d'anticipo sui cultori del diritto amministrativo, la risposta di Hobbes è data dal "silenzio assenso" del sovrano. Con le parole del *Leviatano*, "quando una consuetudine che duri da molto tempo acquista l'autorità di legge, non è la lunghezza del tempo che le conferisce autorità, ma la volontà del sovrano manifestata dal silenzio (perché il silenzio è talvolta indice di consenso), ed è legge solo finché dura il silenzio del sovrano su di essa" (Hobbes ed. 1992: 220-221).

Il secondo problema ha invece a che fare con la regressione all'infinito che la doppia condizione di validità, illustrata sopra, innesca. Postulata la legge come fonte di validità delle norme ad essa sottordinate, sorge infatti il problema che anche quella legge, per esser valida, deve essere sottoposta al test della doppia condizione di validità. Per cui, da un lato, una legge è tale soltanto se essa è posta in essere da chi ne ha la competenza; ma, d'altro canto, tale competenza rinvia necessariamente a un livello sovraordinato dell'ordinamento che è, poi, definito dal piano costituzionale: nel caso dell'Italia, si tratta dell'articolo 70 e seguenti della Carta repubblicana. Lasciando qui da parte le questioni di merito e, cioè, il sindacato di costituzionalità delle leggi (v. sopra § 3.4.1), sorge tuttavia il problema: a che titolo, a sua volta, la Costituzione è valida?

La risposta di Kelsen è stata di postulare, o presupporre sul piano logico, una norma ulteriore a chiusura del sistema, detta anche *Grundnorm* o norma fondamentale. Di qui, si può dire che la costituzione sia valida e, pertanto, doti di validità le leggi ordinarie che, a loro volta, dotano di validità gli atti e provvedimenti amministrativi, se e solo se, con la norma fondamentale, "si postula che ci si debba comportare così come hanno ordinato l'individuo o gli individui che hanno dettato la prima costituzione. Questa è la norma fondamentale dell'ordinamento giuridico in considerazione" (Kelsen ed. 1959: 116). Con la più sintetica formulazione della *Dottrina pura del diritto*, sul piano del disposto della norma fondamentale, "bisogna comportarsi così come prescrive la Costituzione" (Kelsen ed. 1966: 226).

Sul piano logico, Kelsen ritiene così di avere troncato la regressione all'infinito in ragione di una norma che, a differenza di tutte le altre norme dell'ordinamento, a partire dalla costituzione, non è posta, bensì presupposta. Ancora una volta con le sue parole, "la norma fondamentale è la fonte comune della validità di tutte le nor-

me appartenenti allo stesso ordinamento; è il fondamento comune della loro validità. L'appartenenza di una certa norma ad un certo ordinamento riposa sul fatto che il fondamento ultimo della sua validità è la norma fondamentale di questo ordinamento" (Kelsen ed. 1966: 219).

Su queste basi, torniamo significativamente ai paradossi logico-matematici visti a proposito di Gödel, Turing e Chaitin (v. § 2.1.1). In quella sede, come si ricorderà, il genio di Gödel è consistito nel fatto di tradurre nel linguaggio della meta-matematica il classico paradosso del mentitore cretese che afferma di se stesso "io dico il falso", salvo poi scoprire, sul piano logico, che questa classe di proposizioni non è né vera né falsa. Or bene, allo stesso modo, i cultori della materia si sono peritati di spiegare che anche la costituzione, in quanto fonte delle fonti del sistema, non può essere né valida né invalida, ovvero, essa non solleva problemi di validità giuridica ma, se mai, questioni di legittimità politica (me ne occupo in Pagallo 2002: 42).

Del resto, la conclusione è suffragata da un esperto di paradossi logici, l'illustre filosofo inglese Bertrand Russell (1872-1970). Trentenne, egli spedì una lettera a un altro grande logico, Gottlob Frege (1848-1925), che stava allora ultimando i *Principi di aritmetica* (1903), con cui il matematico tedesco sperava di essere finalmente giunto a una coerente sistemazione della teoria dei numeri in chiave logica che, in retrospettiva, possiamo ritenere "l'antenata di tutti i linguaggi di programmazione comunemente usati al giorno d'oggi" (Davis 2003: 75). Nella lettera del 16 giugno 1902, Russell metteva a soqquadro gli "insiemi di insiemi" di Frege, per via del paradosso sugli insiemi degli insiemi che non appartengono a sé: se, poniamo, il barbiere è colui il quale fa la barba a tutti coloro i quali non si fanno la barba in un dato villaggio, chi fa la barba al barbiere?![4]

Nei *Principia Mathematica* che, tra il 1910 e il '13, Russell venne pubblicando con Alfred N. Whitehead (1861-1947), la soluzione è che "qualsiasi cosa coinvolga tutti i membri di un insieme non può essere un membro dell'insieme" (ed. 1960, vol. I: 37).

Tuttavia, come riferito fin dal primo capitolo (§ 1.1.1), si dà il caso che il diritto sia eminentemente un sapere pratico. Per cui, anche a concedere, come ammetto, per via logica, che si applichi alla costituzione la soluzione di Russell al paradosso del barbiere, rimane nondimeno l'ulteriore problema che, onestamente, anche Kelsen riconosce: sul piano concreto, la validità della teoria relativa alla norma fondamentale ha senso soltanto se riferita ad un ordinamento efficace nelle sue grandi linee. Ancora con le parole della *Dottrina pura del diritto*, "l'efficacia dell'ordinamento giuridico come totalità e l'efficacia di una singola norma giuridica sono condizioni di validità non meno di quanto lo sia l'atto con cui si statuisce la norma stessa; e l'efficacia è condizione nel senso che un ordinamento giuridico, considerato come totalità, ed una singola norma giuridica non possono più considerarsi validi, quando cessano di essere efficaci" (Kelsen ed. 1966: 241).

Giungiamo per questa via a quel fenomeno d'incompletezza con il quale abbia-

[4] Anni addietro uno studente vivace, a lezione, cercò di risolvere il paradosso con l'intervento di una donna barbuta; ma, non è stato sufficiente a salvare il povero barbiere che, se intende farsi la barba, allora non può radersi e, viceversa, se non si rade, allora può farsi la barba.

mo cominciato a misurarci fin dal § 2.1.3 e, poi, in § 2.3.1. In questa sede, si tratta d'integrare la definizione standard di fonte, con le cosiddette fonti *extra* e *contra ordinem*.

### 4.1.1. *La definizione integrata di fonte*

La definizione standard delle fonti del diritto come meta-norme di produzione normativa previste dall'ordinamento, va integrata con tutti quegli atti o fatti che, affianco alle fonti formali (*extra ordinem*), o nonostante queste ultime (*contra ordinem*), sono in grado di produrre di per sé diritto in un sistema dato. In altri termini, abbiamo a che fare con un "fatto che per forza propria si traduce in norma" (Paladin 1996: 19).

Più in particolar modo, possiamo pensare a quattro diverse accezioni:

a) un fatto o atto che, pur difforme dal modello previsto dal sistema legale delle fonti, tuttavia, "realizzi il suo scopo" (Paladin 1996: 447);
b) i tipi di fonte che, non previsti affatto dall'ordinamento, si affiancano di fatto al sistema legale delle fonti;
c) quei fatti o atti che previsti dall'ordinamento, sia pure non alla stregua delle fonti, al pari delle fonti legali producono diritto nel sistema;
d) la "serie di fattori estranei e irriducibili, rispetto a quelli prefigurati dall'ordinamento già in vigore" (Paladin 1996: 450), che coincidono con le soluzioni di continuità istituzionale, come nel caso delle rivoluzioni (§§ 3.1.1 e 3.1.3.1), che talora si registrano nella vita costituzionale degli stati.

Naturalmente, secondo gli auspici di Livio Paladin, "al fatto che per forza propria si traduce in norma bisogna riconoscere un decisivo rilievo nei soli momenti di crisi radicale degli Stati, cui le forme ordinarie di creazione del diritto non riescano a far fronte. Viceversa, nella quotidiana esperienza degli ordinamenti statali, giudici, operatori giuridici, comuni cittadini e sottoposti in genere si trovano alle prese con le sole fonti legali, istituite e riconosciute come tali dagli ordinamenti stessi; mentre i fattori che tanti giuristi amano più volte definire quali fonti *extra ordinem* non sono altro che atti o comportamenti illegittimi o illeciti" (*op. cit.*, 19).

Tuttavia, ci siamo soffermati sulla necessità di integrare la definizione standard di fonte con le fonti *extra* o *contra ordinem* del diritto, per tre motivi.

Il primo è storico: se, nelle pagine precedenti, si è già fatto cenno alle rivoluzioni inglese, nordamericana e francese, nel corso del presente capitolo dovremo dar conto di processi di lunga durata, riassumibili nel modello relativo al sistema antico e medioevale delle fonti del diritto, cui ha fatto séguito il paradigma di Westfalia, fino all'odierno stato dell'arte. Va da sé che questi mutamenti sono avvenuti, il più delle volte, tramite fonti *contra* o, quanto meno, *extra ordinem*.

Il secondo motivo d'interesse è scientifico: esso dipende non solo da motivi di completezza espositiva, ma dai fenomeni d'incompletezza esaminati in precedenza in termini di complessità teorica (§ 2.1.3).

Il terzo punto è filosofico e riguarda il modo in cui dobbiamo intendere la natura del diritto, stretto tra il principio di validità e l'efficacia di Kelsen. Nei limiti di questo libro, si tratta di capire il nesso tra l'intento regolativo del diritto come meta-

tecnologia (v. § 1.1.3), e l'impatto della rivoluzione tecnologica sul diritto (v. figura 4 in § 1.4).

Ma, prima di procedere con l'analisi su questi tre versanti d'indagine, converrà aprire una breve digressione e concentrarsi su un particolare aspetto dell'odierno sistema delle fonti che, spesso, risulta ostico ai giuristi della tradizione del diritto continentale europeo: vale a dire, il tema della giurisprudenza come fonte del diritto.

### 4.1.2. *La giurisprudenza come fonte del diritto*

Che la giurisprudenza sia fonte del diritto nella tradizione anglo-americana di *common law* e, in genere, nei sistemi imperniati sul dualismo di gubernaculum e iurisdictio esaminato nel capitolo precedente, è fuori discussione. Se mai, il problema si pone per la tradizione continentale europea di *civil law*, per la quale si profila il seguente dilemma:

– o, come vuole appunto questa tradizione, la giurisprudenza non è fonte del diritto; ma allora, davanti all'evidenza che la giurisprudenza è a tutti gli effetti un fattore di produzione normativa dell'ordinamento, bisogna concludere che la stessa è una fonte *extra* o addirittura *contra ordinem*;

– oppure, occorre arrendersi all'evidenza e abbracciare la tradizione dualista.

Per cogliere ulteriormente i termini del problema, torna utile l'esempio della Costituzione italiana, muovendo dal tenore del secondo comma dell'articolo 101 che stabilisce la soggezione dei giudici soltanto nei confronti della legge. L'articolo può essere innanzitutto inteso come corollario del principio di sovranità popolare che deriva, come suol dirsi, dal "combinato disposto" del primo comma dell'articolo 101 con il secondo comma del primo articolo della Carta fondamentale. In nome della sovranità popolare, il popolo esercita infatti detta sovranità ora in forma diretta, ora indiretta: nel primo caso, si hanno le procedure referendarie previste dagli articoli 75 e 138, così come l'elezione degli organi legislativi stabilita dagli articoli 56, 58 e 122. L'esercizio indiretto della sovranità, invece, si svolge ora attraverso la legislazione ordinaria e costituzionale del Parlamento ai sensi degli articoli 70 e 138, ora mediante la legislazione regionale di cui al 117, ora tramite il controllo politico che il Parlamento è chiamato a svolgere nei confronti dell'attività del Governo stante gli articoli 77 e 94. Sulla base di queste disposizioni, ne consegue che "la magistratura costituisce un ordine autonomo e indipendente da ogni altro potere" dello stato e "le nomine dei magistrati hanno luogo per concorso" – come recitano i primi commi degli articoli 104 e 106 – ma proprio perché l'attività dei giudici, chiamati ad applicare la legge cui sono per l'appunto sottoposti ai sensi del 101, viene intesa come scevra da ogni titolo di rappresentanza politica.

Nei decenni successivi all'entrata in vigore della Costituzione, la dottrina è stata più volte chiamata a precisare il significato delle espressioni letterali che compaiono nel secondo comma dell'articolo 101. La nozione di "legge" è stata così affinata in senso formale, comprendendo sia le leggi ordinarie e costituzionali approvate dal Parlamento, sia i risultati dei referendum popolari e gli atti aventi per l'appunto forza di legge ai sensi degli articoli 75 e seguenti della Costituzione. Inoltre, gli studiosi hanno molto discusso su chi siano i "giudici" del 101 – distinguendosi tra il profilo

soggettivo del titolo dell'autorità giurisdizionale e l'oggettivo esercizio di questa funzione – giungendo però alla conclusione che tra questi giudici non vadano annoverati quelli della Consulta. Sebbene, con la ridondanza che deriva dal sistematico accostamento degli articoli 134, 135 e 137, la Corte sia composta da "giudici", chiamati a "giudicare controversie" tramite "giudizi", questi giudici non sono riconducibili al genere del 101 perché, secondo il tenore del 134, la Consulta, tra le altre cose, è chiamata a giudicare "sulle controversie relative alla legittimità costituzionale delle leggi e degli atti, aventi forza di legge, dello Stato e delle Regioni".

La conclusione, peraltro condivisibile, ha tuttavia dato origine a un duplice paradosso. Il primo riguarda chi, sulla scia di Kelsen, individua nella Corte costituzionale l'organo di chiusura del sistema e, nondimeno, anche di fronte alle sue sentenze *erga omnes* additive, manipolative o normative, insiste nell'escluderle dal novero delle fonti. Nei confronti di quest'ultima soluzione, si obbietta che essa produrrebbe una forzatura, se non addirittura una vera e propria violazione dello spirito e della lettera dell'articolo 136 della Costituzione; ciò che, a sua volta, comporterebbe una modifica tacita della stessa Carta repubblicana. Per tornare alle tesi di Paladin, accreditare l'immagine della Corte come fonte dell'ordinamento, significherebbe infatti presentarla come un "colegislatore", privo di "legittimazione democratica", "falsando per ciò solo la natura esclusivamente negativa del controllo di costituzionalità delle leggi e degli atti equiparati" (Paladin 1996: 457). La difficoltà, in altri termini, può anche assumere la forma dell'interpretazione: "come si può concepire, cioè, che il giudice al quale si affida la chiusura del sistema, sul piano dell'interpretazione costituzionale, sia quello che produce – con le sue stesse sentenze – una serie di norme incompatibili con la Costituzione?" (*op. cit.*, 458).

Il secondo paradosso va colto sullo sfondo del sindacato di costituzionalità delle leggi e riguarda la funzione della magistratura ordinaria, adempiuta nel nome del popolo sovrano e, come tale, sottoposta all'attività politico-legislativa parlamentare. Alla tesi della giurisprudenza (ordinaria) come fonte del diritto è contrapposta sia la natura politica della legislazione, sia la dottrina della legge come funzione primaria e originaria del sistema giuridico. Dal primo punto di vista, si obbietta che al pari dei giudici costituzionali, i giudici ordinari non sono provvisti del potere d'iniziativa ma, piuttosto, risultano vincolati dai principi del *petitum* e, quindi, del *nec ultra petita*. Dal secondo punto di vista, si rileva che, diversamente da ciò che viene previsto per le leggi, non solo ricade sui giudici l'obbligo di motivazione dei provvedimenti da loro presi, con la necessità di indicare le norme applicate nel caso considerato; ma, è anche contemplata l'ulteriore possibilità, sancita dal secondo comma dell'articolo 111 della Costituzione, di ricorrere innanzi alla Suprema Corte di cassazione per ogni caso di "violazione di legge" da parte dei giudici ordinari e speciali. In che senso, dunque, è lecito parlare della giurisprudenza come fonte del diritto, se non come fonte *extra* o *contra ordinem* dell'ordinamento?

In realtà, sebbene quest'ultima tesi goda ancora di grande popolarità in certi ambienti politici italiani, basterebbe far caso ai tre scenari illustrati in precedenza, tra gubernaculum e iurisdictio (v. § 3.4.1), per comprendere come mai, anche nella tradizione continentale di *civil law*, la giurisprudenza sia fattore di produzione normativa nel sistema giuridico. Lasciando da parte i casi in cui gli organi della iurisdictio sono chiamati a sindacare la legittimità delle scelte politiche prese dagli organi

del gubernaculum, si pensi ai problemi che tali scelte politiche, fissate in una legge o in uno statuto, possono lasciare nondimeno aperti, oppure a tutte le controversie in cui il legislatore non ha saputo, o non ha voluto, intervenire. Tra gli innumerevoli esempi possibili, mi limito a ricordare quello della tutela della riservatezza in Italia, dove, per anni, il parlamento si è guardato bene dal legiferare. Siccome, però, i problemi di tutela sono sorti egualmente, si è dovuto colmare questa lacuna secondo i principi ermeneutici suggeriti dall'articolo 12 delle preleggi [5], che autorizza il ricorso all'analogia, salvo in materia penale (articolo 14), nonché ai principi generali dell'ordinamento, ovviamente declinati in chiave costituzionale.

Così, se in un primo momento, con la sentenza 4487 del 22 ottobre 1956, la Cassazione ha negato l'esistenza di un autonomo diritto alla riservatezza, sette anni dopo essa ha cambiato avviso, ammettendo "l'esistenza nel nostro ordinamento di un diritto assoluto di libera determinazione nello svolgimento della personalità, diritto che può ritenersi violato quando si divulgano notizie della vita privata di un soggetto senza il suo consenso, almeno implicito" (sentenza 990 del 20 aprile 1963). Dieci anni dopo, con la fondamentale pronuncia della Corte costituzionale 38 del 14 aprile 1973, si è espressamente incluso il diritto alla riservatezza tra i diritti inviolabili dell'uomo che la Costituzione garantisce al pari del decoro, onore, rispettabilità, intimità e reputazione. Dopo di che, con la sentenza 2129 del 27 maggio 1975, la Corte di cassazione si è uniformata alla decisione della Consulta, riconoscendo del pari l'esistenza di un autonomo diritto alla riservatezza nell'ordinamento giuridico italiano.

Su queste basi, così come in altre circostanze, si è creato fisiologicamente diritto all'interno del sistema, senza per questo dover bussare alle porte del legislatore dormiente. Laddove, poi, il legislatore si svegli, come occorso con la prima normativa italiana in materia di tutela dei dati personali, ossia la legge 675 approvata dal Parlamento di Roma il 31 dicembre 1996, è altamente probabile che non mancheranno i casi in cui la giurisprudenza sarà nuovamente chiamata a produrre diritto, affrontando volta per volta i problemi che l'intervento del legislatore ha lasciato aperti. Si tratta in fondo di quella dialettica delle istituzioni, tra gubernaculum e iurisdictio, su cui siamo venuti insistendo fin dall'introduzione del capitolo precedente (v. ivi figure 14 e 15).

## 4.2. *Il modello di Westfalia*

Si riassume spesso con la formula del "modello di Westfalia" il sistema delle fonti invalso negli ordinamenti giuridici occidentali per circa tre secoli, vale a dire dal trattato di Westfalia (1648), appunto, fino grosso modo alla fine della seconda guerra mondiale (1945). Al pari dell'uso delle metafore, anche i modelli storici vanno però impiegati con un grano di sale, servendo in questo caso a cogliere le discontinuità istituzionali, politiche e giuridiche, le quali si danno man mano nel corso dei secoli, senza per questo pretendere di offrire una piena aderenza tra modello e realtà.

Sul piano teorico, il modello di Westfalia può essere convenientemente illustrato

[5] Il riferimento va alle disposizioni preliminari al codice civile italiano del 1942, tuttora vigenti.

con i principi della filosofia giuridica e politica di Hobbes, su cui v. § 2.1.2.1. Ma, nello stesso modo in cui abbiamo visto esserci vere e proprie contraddizioni nel pensiero di Hobbes, così, a proposito del modello di Westfalia, non si vuole certo suggerire né che gli ordinamenti giuridici europei del 1648 fossero già imperniati sui criteri hobbesiani del giuspositivismo e del monopolio delle fonti da parte del sovrano, né che la crisi del modello tre secoli più tardi abbia fatto svanire all'improvviso gli assunti di base dello schema. Facendo riferimento al modello di Westfalia, l'idea è piuttosto quella di apprezzare sia il profondo mutamento occorso rispetto al precedente sistema medioevale delle fonti, sia l'odierna posta in gioco con le fonti delle società ICT-dipendenti.

Alla luce del pensiero di Hobbes, vediamo dunque, innanzitutto, cosa cambi tra medioevali e moderni.

### 4.2.1. *Il pluralismo medioevale*

È proverbiale l'intricata ragnatela di ordinanze, statuti, carte, leggi, consuetudini, usi, glosse, sentenze e commenti dottrinali che, sui vari fronti del diritto comune della tradizione romana, del diritto locale e canonico, e ai diversi livelli dell'impero, dei re, dei nobili sul proprio territorio, e con le città e i mercanti a difesa delle rispettive autonomie, formano il modello medioevale delle fonti. A rigore, è difficile parlare in senso proprio di un sistema ed è significativo che il Lord Cancelliere inglese, Francis Bacon, proponesse già ai suoi giorni di razionalizzare il diritto del proprio paese con un codice. Ancor più significativo è, poi, il fatto che, una volta estromesso dalla scena politica a séguito del primo processo per *impeachment* della storia costituzionale moderna (1621), Bacon, ritiratosi nel frattempo a vita privata, amasse trascorrere buona parte del suo tempo in compagnia di un giovane segretario arrivato da Malmesbury, Thomas Hobbes!

L'allievo avrebbe ben presto superato il maestro, quanto meno nel campo della filosofia giuridica e politica: mentre Bacon viene talora celebrato ancora oggi come uno dei padri nobili della scienza naturale e sperimentale moderna, Hobbes, come detto (v. § 2.1), viene spesso ricordato come il padre della scienza giuridica e politica moderna (Bobbio 1989a). È dunque a Hobbes che dobbiamo ricorrere per chiarire il "modello di Westfalia" e schematizzare, per quanto possibile, il precedente reticolo delle fonti medioevali.

In particolare, i capisaldi della dottrina di Hobbes invitano a riflettere su tre punti principali: il primo concerne la caratteristica pluralità delle fonti in era medioevale, in contrasto con il monismo propugnato dal filosofo inglese. Alle tradizionali coppie di fonti atto e fonti fatto, legislazione e consuetudini, ossia, nel linguaggio di Hayek, tra taxis e kosmos, va qui aggiunto il "formante dottrinale" (Sacco 2007). A partire dalla riscoperta dei testi giustinianei e l'opera del sommo giurista Irnerio (1050-1125 ca.), con la scuola dei glossatori e, successivamente, dei commentatori, tra cui spicca Bartolo da Sassoferrato (1313-1357), venne formandosi un diritto per via dottrinale che, nell'arco di un paio di secoli, avrebbe posto le basi per quel diritto comune, a ispirazione romana, vigente in quasi tutto il continente europeo. All'atto pratico, ciò significa che di tanto in tanto, per dirimere una controversia in Polonia, o in Ungheria, i dottori del luogo si recavano presso una delle prestigiose

università italiane, come Bologna, fondata nel 1188, o Padova (1222), per consultare le glosse d'Irnerio, i commenti di Bartolo, o di Baldo degli Ubaldi (1327-1400). Si è trattato di una gloriosa tradizione che, per molti versi, si sarebbe formalmente spezzata solo con il codice napoleonico (1804); e che, nondimeno, trova ancora in pieno Ottocento espressione nella maestosa opera di Savigny, il *Sistema del diritto romano attuale*, pubblicato in otto volumi tra il 1840 e il '49. Qui, troviamo la ricordata tesi che lo spirito del popolo – beninteso, mediato dalla sapienza del giurista – è la fonte per eccellenza del sistema giuridico.

Il secondo punto da rimarcare, riguarda il dualismo costitutivo di gubernaculum e iurisdictio, in opposizione alla sovranità unica e indivisibile che caratterizzerà la teoria dei moderni. Anche a privilegiare, rispetto alla tradizione inglese di Bracton e di Fortescue (v. § 3), quella continentale che fa capo ai glossatori e, in specie, ad Azzone da Bologna (1150-1225 ca.), per cui il monarca che non riconosce superiori nel proprio regno deve essere considerato alla stregua dell'imperatore, rimangono tuttavia evidenti le differenze con la moderna nozione di sovranità "sciolta dalle leggi" (v. § 2.1.2.1). Quest'ultima idea non può che cozzare con l'interpretazione giuridica della politica data dai glossatori, in quanto, se i poteri che la coscienza dell'epoca assegnava all'imperatore dovevano ora essere riconosciuti al re, questi poteri non erano *legibus solutus*, ma suggeriscono piuttosto un modo nuovo d'intendere il rapporto tra diritto comune e diritto proprio sul piano delle fonti. Riconosciuta la preminenza del diritto proprio di ciascun ordinamento particolare, il diritto comune assumeva, cioè, "una funzione sussidiaria di regolatore e coordinatore supremo" (Calasso 1957: 23). A conferma della tesi, basterebbe far caso alle incertezze del primo teorico moderno della sovranità, il giurista francese Jean Bodin (1530-1596): per quanto, ne *I Sei Libri dello Stato* (1576), egli insista più volte sull'"assolutezza" della sovranità, per cui "il punto più alto della maestà sovrana sta nel dar legge ai sudditi in generale e in particolare, senza bisogno del loro consenso" (*op. cit.*, ed. 1964: 374), Bodin si perita pur sempre d'individuare nella legge divina, in quella naturale e nelle altre leggi fondamentali del regno, quali la legge salica, con l'inalienabilità del territorio o l'impossibilità di abolirne gli Stati, altrettanti limiti al potere sovrano (*op. cit.*, 357-368).

Il terzo motivo di differenza tra medioevali e moderni, infine, ha a che fare con la natura personale e fiduciaria delle relazioni giuridiche, basate sullo status individuale, più che sul criterio territoriale sancito dal modello di Westfalia, incardinato sul principio della sovranità degli stati. Rispetto alla istituzionalizzazione moderna delle relazioni giuridiche, con la distinzione tra interno ed esterno, tra diritto nazionale e diritto straniero, tipica di Hobbes, salta all'occhio la porosità della distinzione tra diritto proprio e diritto comune nel sistema medioevale delle fonti, a cui va ad aggiungersi l'universalismo del diritto canonico nei suoi controversi rapporti con l'imperatore e i re. Per un verso, il diritto proprio non va inteso necessariamente dislocato in un dato territorio ma, anzi, può assumere valenza trasversale: come attesta eloquentemente il caso del diritto speciale dei mercanti, o *lex mercatoria*, il genitivo dell'espressione va declinato in senso soggettivo, non oggettivo, e cioè come diritto che i mercanti, ovunque siano, danno a sé. D'altro canto, per quanto vadano forgiandosi le idee moderne di esterno e interno, con la formazione degli stati nazionali e lo scisma protestante, il sistema medioevale delle fonti in tanto tiene, in quanto

reggono i collanti del diritto comune e un'idea altrettanto condivisa di cristianità. Entrato irreversibilmente in crisi il modello con le guerre di religione – *I Sei Libri* di Bodin vengono non a caso pubblicati quattro anni dopo la strage di san Bartolomeo, nel 1572, a Parigi – bisognerà attendere il genio di Hobbes per avere un nuovo, compiuto modello, destinato a orientare politici e giuristi per quasi tre secoli.

Proviamo ora a riassumere i punti chiave del pluralismo medioevale emerso con questi cenni, sulla base di uno schema, i cui riquadri (ossia gli osservabili del modello) andranno di volta in volta precisati:

| Fonti medioevali | Diritto Proprio | Diritto Comune | Diritto Canonico | Diritto Regio |
|---|---|---|---|---|
| Gubernaculum | | | | |
| Iurisdictio | | | | |
| Kosmos | | | | |
| Scienza Giuridica | | | | |

Tavola 1: *Il pluralismo medioevale*

Per quanto abbia cercato di comprimere con le istanze metodologiche illustrate in § 2.1.2, l'informazione necessaria per cogliere la complessità del sistema medioevale delle fonti, mi rendo conto della semplificazione di uno schema che, temo, farà storcere la bocca a più di uno storico del diritto. Per esempio, sul piano orizzontale della tavola, può obiettarsi come manchi un riferimento autonomo al diritto imperiale, qui assorbito sotto quello regio, mentre il diritto dei mercanti viene presentato, non senza qualche forzatura, sotto la nozione di diritto proprio. Invece, sul piano verticale della tavola, gubernaculum e iurisdictio sono distinti dal kosmos, e non, al modo di Hayek, presentati sotto l'unica etichetta di taxis: mentre, nel corso del capitolo precedente, abbiamo spiegato le ragioni della loro irriducibilità, si potrebbe eccepire che anche la nozione di kosmos andrebbe a sua volta distinta, come minimo, tra consuetudini e autonomia contrattuale delle parti.

Tuttavia, occorre pure avvertire che l'intento dello schema non è di rendere tutta la complessità del sistema medioevale delle fonti; ma, piuttosto, di cominciare a cogliere sin d'ora la distanza che corre tra quest'ultimo sistema e il modello di Westfalia.

Per fortuna, la matematica soccorre al fine di evitare che lo schema appaia come una sorte di "letto di Procuste", in cui le fondamentali differenze tra, poniamo, diritto proprio e diritto dei mercanti, tra diritto imperiale e diritto regio, tra consuetudini e contratti, siano semplicemente ignorate. Basta considerare i rapporti tra gli osservabili della nostra tavola come un numero "n" di oggetti, con lunghezza "k" presa a coppie "c", come nello schema, oppure a triple "t", ecc.; per cui è dato calcolare le combinazioni semplici C, ossia le variabili del modello, secondo la formula:

$$C_{n,\, k(c,\, t,\, ecc.)} = n! \,/\, k!\,(n-k)!$$

Su queste basi elementari[6], s'innesta un duplice accorgimento. Da un lato, occorre evitare di enumerare le combinazioni prive di particolare pertinenza giuridica, ossia quelle a coppia. Si pensi ad esempio al rapporto tra gubernaculum e iurisdictio privo di ogni riferimento al diritto proprio o comune, oppure al rapporto tra diritto canonico e regio sganciato da ogni ulteriore richiamo alle fonti del sistema. Di qui, dobbiamo enumerare gli 8 osservabili della tavola 1 a triple, domandandoci che ruolo abbia il gubernaculum tra diritto proprio e comune, quale il nesso tra gubernaculum e iurisdictio nell'ambito del diritto canonico o regio, e così via.

D'altro canto, reso più concreto lo schema su base n=8 e k=3, bisogna eliminare ulteriormente le triple tra gli elementi che compongono gli assi orizzontali e verticali della tavola 1. Sebbene si possa astrattamente considerare ora il rapporto tra diritto proprio, comune e canonico, ora il rapporto tra gubernaculum, iurisdictio e kosmos, e via di questo passo, mancherebbe la concretezza che si dà solo incrociando gli osservabili dei due assi. In altri termini, la combinatoria a triple (k=3) riguarda soltanto una coppia per ciascun asse, contestualizzata nel rimando a un osservabile dell'altro.

In ragione di questi accorgimenti, la complessità che discende dagli 8 osservabili della tavola 1, da 14 combinazioni a base k=2, passa così a 56 con k=3, che a loro volta diventano 48 se eliminiamo le triple interne agli assi verticali e orizzontali della tavola.

Se, poi, accontentando gli esperti di diritto medioevale, si ritiene che, all'interno del kosmos, sia il caso di sottolineare la specificità dei contratti rispetto alle consuetudini, passando da 8 a 9 osservabili nello schema, si va da 14 a 18 combinazioni con k=2. Ma, più opportunamente, enumerati con triple, si passa da 56 a (84–14=) 70!

Naturalmente, come riferito più sopra in tema di complessità e teoria delle reti (§ 2.2.2.1), troveremmo anche nel reticolo delle fonti medioevali ciò che Herbert Simon definiva una "struttura gerarchica ben definita". È la ragione per cui, nei libri di storia, ci sono validi motivi che hanno spinto gli studiosi ad attrarre l'attenzione sul rapporto tra diritto proprio e diritto comune nei termini della scienza giuridica, tra gubernaculum e iurisdictio in certi ordinamenti regi, tra diritto regio e diritto canonico nei termini del gubernaculum, e via discorrendo.

Tuttavia, senza dilungarci sulle combinazioni a tre che hanno intrattenuto, nel corso dei secoli, gli storici del diritto, è forse il caso di passare ora allo studio del modello di Westfalia, alla luce di questi elementari calcoli di complessità.

### 4.2.2. *La semplicità di un modello*

I principi del modello di Westfalia possono essere desunti, come detto, dalla teoria giuridica e politica di Hobbes: di qui, per ciascuno dei tratti distintivi del sistema medioevale delle fonti, si assiste a una drastica semplificazione.

In primo luogo, rispetto al precedente pluralismo delle fonti, si passa idealmente a uno stretto monismo, dato che né la giurisprudenza, né le consuetudini, né le opinioni della dottrina possono essere considerate legittimi fattori produttivi del siste-

[6] Per il lettore arrugginito in matematica, ricordo che l'annotazione "n!" significa che, dato un numero "n", lo stesso va moltiplicato a decrescere, per cui, essendo "n", poniamo 5, segue che "5!" significhi "5x4x3x2". Stesso calcolo, va da sé, vale per "(n-k)!"

ma giuridico. Anzi, insiste più volte Hobbes nel corso della sua opera, è proprio questo pluralismo delle fonti a rappresentare una delle principali ragioni che conducono gli uomini alla condizione ferina dello stato di natura: più che dalla mancanza di regole, tale stato spesso dipende dal fatto che tutti ritengono di avere ragione.

In secondo luogo, rispetto al dualismo tra gubernaculum e iurisdictio, sia pure nelle forme attenuate dei glossatori e commentatori del continente europeo, è un dato di fatto che molti sistemi giuridici abbiano finito per adottare un approccio giuspositivistico e centralista. Ciò significa che l'unico diritto che vale, nella società civile, è quello stabilito dalla volontà del sovrano, secondo una posizione che, già prima di Hobbes, Bodin aveva sostenuto nei *Sei Libri*: "la sovranità appartiene completamente, senza alcuna spartizione, ai re d'Inghilterra, e gli stati [Parlamento] non vi hanno niente a che vedere" (*op. cit.*, 374).

In terzo luogo, rispetto all'universalismo medioevale, gli ordinamenti si fondano sul principio di territorialità dello stato che definisce la reciproca sfera di non ingerenza. Al monismo interno sul piano delle fonti, corrisponde così un dualismo sul piano di ciò che nel corso dei secoli XVI e XVII, al posto del vecchio diritto comune, sarebbe invalso come diritto pubblico europeo; e che, a partire dall'Ottocento, con il crescente ruolo degli Stati Uniti d'America, si sarebbe cominciato a chiamare con la fortunata formula di Jeremy Bentham (1748-1832), "diritto internazionale". Al monopolio legale della forza riservato al sovrano sul fronte interno, fa da controcanto il ruolo dei sovrani come unici soggetti del diritto internazionale. Come leggiamo nel capitolo diciottesimo del *Leviatano*, "inerisce alla sovranità il diritto di fare la guerra e la pace con le altre nazioni e gli altri Stati; vale a dire di giudicare sia quando l'uno o l'altra convenga al bene pubblico" (Hobbes ed. 1992: 150).

In ragione di questi tre punti, possiamo ricavare un nuovo schema che esplicita la razionalizzazione del diritto a lungo invocata dai moderni: dalle almeno 56 variabili del sistema medioevale delle fonti, si passa infatti a 3 osservabili e 2 sole variabili!

| Le fonti di Westfalia | Diritto Interno | Diritto Internazionale |
|---|---|---|
| Volontà del Sovrano | | |

Tavola 2: *Il monismo nelle fonti dei moderni*

A ribadire la straordinaria compressione teorica del modello, si tenga presente che lo schema, imperniato sul principio di sovranità degli stati su base territoriale, dà conto sia della versione assolutistica del contratto sociale di Hobbes (§ 2.1.2.1), sia della versione democratica approntata da Rousseau (§ 3.1.2), sia delle letture monistiche della Carta repubblicana italiana ricordate in precedenza (§ 4.1.2). Ne è conferma, d'altro lato, che l'interpretazione "dualistica" del rapporto tra diritto interno e diritto internazionale non sia soltanto appannaggio dei "realisti", in opposizione ai "globalisti" (§ 3.3.2); ma, è il modo in cui tuttora la Corte costituzionale italiana intende tale rapporto, anche quando il termine di raffronto è il diritto europeo con le sentenze della Corte di giustizia UE.

Inoltre, la compressione teorica del modello non viene meno, neanche nel caso in cui l'ordinamento giuridico considerato, al suo interno, accolga la tradizione dualistica di gubernaculum e iurisdictio. È il caso, emblematico, degli Stati Uniti d'America (§ 3.2); e, in parte, del contratto sociale di Locke (§ 3.1.1). In questo modo, il modello passa da 3 a 4 osservabili, ma con 3 sole variabili!

| Le fonti di Westfalia | Diritto Interno | Diritto Internazionale |
|---|---|---|
| Gubernaculum | | |
| Iurisdictio | | X |

Tavola 3: *Il dualismo nelle fonti dei moderni*

La ragione per la quale, nella terza tavola, la variabile tra diritto internazionale e iurisdictio è infatti esclusa ("X"), dipende dagli assunti del modello di Westfalia: siccome gli unici soggetti del diritto internazionale sono gli stati sovrani nazionali rappresentati dagli organi di governo, segue che il ruolo della iurisdictio sia limitato al versante interno delle istituzioni. Tanto le difficoltà della Corte permanente di arbitrato internazionale o Tribunale dell'Aia (1899), quanto l'esperienza fallimentare della Corte permanente presso la Società delle Nazioni (1919-1922), mostrano in fondo i limiti della iurisdictio all'interno di questo modello. Ciò non ha impedito a uno studioso americano di sostenere, *Nei migliori angeli della nostra natura*, che il monopolio degli stati sovrani sull'uso legittimo della forza sia da annoverarsi tra i "fattori storici" che "hanno condotto alle multiple diminuzioni della violenza", inibendo l'impulso per la vendetta, disinnescando la tentazione di attacchi profittatori o aggirando faziosità auto-referenziali (Pinker 2012).

Ma, se anche così fosse, rimane il disastro e l'orrore di due conflitti mondiali che, specie a partire dal secondo dopoguerra, avrebbero condotto alla messa in mora di un pilastro del modello di Westfalia, vale a dire il limite posto ai poteri della iurisdictio nel campo del diritto internazionale. A partire dai processi per i crimini di guerra svoltisi a Norimberga (1946-1947), e a Tokyo (1946-1948), si comincerà a sottoporre a giudizio l'operato dei sovrani nazionali, secondo uno sviluppo che, specie dopo la fine della guerra fredda (1989), condurrà al Tribunale per i crimini di guerra nell'ex-Jugoslavia, istituito il 25 maggio 1993 con la risoluzione 827 del Consiglio di Sicurezza delle Nazioni Unite, al Tribunale di Arusha, in Tanzania, per i crimini commessi nel Ruanda nel 1994, fino al trattato di Roma dell'ottobre 1999 con cui è stata istituita la Corte penale internazionale (ICC), i cui lavori hanno avuto inizio all'Aia il primo luglio 2002.

Non si mira a suggerire in questo modo che il progetto cosmopolitico kantiano abbia avuto il sopravvento sul vecchio modello di Westfalia (si v. §§ 1.1.3 e 3.3.2). A ben vedere, è altamente indicativo che, allo stato, le grandi potenze mondiali, vale a dire Stati Uniti d'America, Cina e Russia non abbiano alcuna intenzione di aderire all'ICC.

Piuttosto, si vuole segnalare come la crisi del modello di Westfalia e di un pilastro del diritto internazionale classico, quale l'immunità riservata ai sovrani nazionali, sia spia di una storia ancor più complessa e intricata. Basti pensare a quanto detto a proposito del processo d'integrazione europea (§ 3.2.2), per cui il nuovo ruolo

della iurisdictio sul piano del diritto internazionale non si è certo limitato ai pur rilevantissimi compiti della giustizia penale, ma si è esteso fino al punto di mettere in gioco la sovranità degli stati membri dell'Unione con i problemi della "competenza della competenza".

Inoltre, tornando agli osservabili e alle variabili del nostro schema (v. Tavola 3), non si tratta soltanto di passare da 3 a 4 variabili del modello; bensì, bisogna recuperare quelle fonti che si ritenevano estinte con il venir meno del sistema medioevale, oppure, dar nome a nuovi tipi di fonti per le quali, come già ai tempi di Bentham, si è dovuto ricorrere all'uso di neologismi, come nel caso del "diritto transnazionale". Cerchiamo dunque di capire il perché della crisi di un modello.

### 4.2.3. *La crisi di un modello*

Imperniato sul principio di sovranità degli stati sovrani nazionali, il modello di Westfalia entra in crisi allorché i suoi protagonisti, ossia, appunto, gli stati, finiscono per apparire progressivamente o "troppo piccoli", o "troppo grandi", rispetto ai problemi da affrontare. Questo processo, più volte notato nel corso degli ultimi decenni, non significa che lo stato sia destinato a sparire ma, piuttosto, a riposizionarsi rispetto a spinte di tipo sia centripeto sia centrifugo, ovvero, che conducono in certi casi verso organizzazioni di stampo sovranazionale, altre volte invece verso il decentramento delle tradizionali organizzazioni statali. In entrambi i casi, è possibile dar conto della crisi del modello di Westfalia nei termini oramai familiari di "complessità" (si v. la figura 5 del capitolo secondo).

Per un verso, sul fronte delle spinte centripete in direzione sovranazionale, la compressione teorica del modello con i suoi 3 o 4 osservabili, e a 2 o 3 variabili, non è più in grado di abbracciare la complessità dei problemi che gli stati sovrani nazionali devono affrontare, poiché questi problemi investono progressivamente la totalità del sistema, vale a dire che aggrediscono gli stati sovrani nel loro complesso. Sono i temi introdotti fin da § 2.3 e, successivamente, illustrati con i nodi dell'integrazione europea (v. § 3.3), con le tesi della Banca Mondiale e del Fondo Monetario (§ 3.3.1), fino alla governance di internet (§ 3.4). Si tratta di un processo che trova, per molti versi, il suo spartiacque nel secondo dopoguerra con il venir meno di uno dei capisaldi del modello di Westfalia, vale a dire l'immunità degli organi sovrani degli stati nazionali (§ 4.2.2), e la nuova stagione delle organizzazioni internazionali, a partire dalla istituzione delle Nazioni Unite (1945).

D'altro canto, sul fronte delle spinte centrifughe che spingono al decentramento, ciò che sfugge alla compressione teorica del modello di Westfalia riguarda la dinamica di rapporti sociali assai più complessi di quanto l'uomo riesca a calcolare o a gestire artificialmente. Qui, il riferimento va in chiave teorica alle considerazioni di Hayek sul kosmos (§ 2.2.1), con la formazione degli ordini spontanei (§ 2.2.2), che possono agevolmente ricondursi ai temi tradizionali degli usi e consuetudini nel sistema delle fonti invalso nel medioevo. Infatti, abbiamo ricordato come Hayek insista sui meccanismi del mercato, con le leggi della domanda e dell'offerta, per chiarire i limiti della taxis e di ogni costruttivismo giuridico, secondo motivi che riconducono allo statuto della *lex mercatoria* come fonte del sistema giuridico medioevale (§ 4.2.1). Si tratta di un percorso che ha indotto qualche studioso a retrodatare la crisi del modello di Westfalia in

chiave di globalizzazione, alla fine del XIX secolo, ossia ai tempi della *belle époque* (Amin 2000). Si pensi a giuristi come Lorenz von Stein (1815-1890), o Maurice Hauriou (1856-1929), che individuavano nel settore del diritto internazionale privato l'ordinamento comune del mercato e dell'economia, "il cui campo d'azione è il mondo", sottolineando l'incidenza determinante del commercio in vista "di un grande spazio unificato federalisticamente" (si v. Schmitt 1991: 300 e 312).

Del resto, questo risorgere degli ordini spontanei e delle consuetudini giuridiche, *sub specie lex mercatoria*, unitamente al riordino istituzionale in corso con la governance europea, ha suggerito a qualche altro autore di proporre questa volta un parallelismo tra il vecchio diritto comune europeo e il nuovo pluralismo nel sistema delle fonti (Coing 1989). In fondo, come diremo nel prossimo paragrafo, uno degli esempi più ricorrenti per illustrare le nuove frontiere del diritto transnazionale, è proprio quello della *lex mercatoria* (Zumbansen 2006).

Nondimeno, anche a supporre tanto il ritorno delle consuetudini sul piano delle fonti del sistema, quanto l'esempio paradigmatico della legge dei mercanti, c'è una buona ragione per cui resistere a simili parallelismi tra l'attuale globalizzazione e la *belle époque*, tra l'odierno assetto delle fonti e il diritto comune europeo. Come riferito a partire dal primo capitolo (§ 1.4), e poi illustrato sia con i mondi piccoli d'internet (§ 2.2.2.1), sia con i profili della sua odierna governance (§ 3.4.2), la ragione consiste nei profili giuridici della "quarta rivoluzione" (si v. la figura 4 in § 1.4). È per questo che, nella parte conclusiva del presente capitolo, il riferimento al nuovo modello delle fonti emerso con la crisi del paradigma di Westfalia, sarà colto all'insegna delle fonti delle società che ho già definito come ICT-dipendenti (§ 1.4.4).

## 4.3. *Le fonti delle società ICT-dipendenti*

Abbiamo concluso il capitolo precedente, esponendo tre criteri per giungere a un appropriato bilanciamento tra rappresentanza politica e decisioni giuridiche nell'odierna governance; criteri che conducevano alla necessità di appurare sia il livello sia le modalità con cui intendere i profili del diritto come meta-tecnologia, secondo ciò che si è avuto modo di illustrare con la figura 3 del § 1.1.3. Riprendendo questo punto con le ragioni della crisi del modello di Westfalia, esposte nel paragrafo precedente, possiamo ora formalizzare la questione con un nuovo schema che, tuttavia, richiede qualche avvertenza preliminare.

In primo luogo, avendo modo di rifarci ancora alle nozioni di "diritto nazionale" o "diritto internazionale", già presenti nel precedente modello delle fonti, ciò lascerebbe supporre una sostanziale continuità tra i due modelli, quello di Westfalia e quello delle società ICT-dipendenti. Sebbene tale continuità sia in qualche modo inevitabile, occorre però sottolinearne sin d'ora la differenza, che dipende dal diverso contesto in cui tali nozioni vanno pensate. Ad esempio, per quanto concerne il diritto internazionale, si è già avuto modo di rimarcare la differenza che corre tra il diritto internazionale classico, i cui unici soggetti erano gli stati nazionali sovrani, sottratti come tali ai poteri della iurisdictio, e le nuove tendenze del diritto internazionale odierno, tra cui va ricordata quella forma inedita che è rappresentata dall'Unione europea (si v. § 4.2.2). Come diremo, la stessa avvertenza vale anche per la

formula del "diritto nazionale" con le sue specifiche modalità d'intervento, per cui, alle forme tradizionali del potere coattivo della legge, riassunto secondo la canonica formula del "se A, allora B", vanno ad aggiungersi nuovi strumenti di disciplina autoritativa o *soft law*.

In secondo luogo, nel distinguere il livello nazionale da quello internazionale, occorre anche ricordare i processi di de-territorializzazione dell'ordinamento, messi in atto dalla rivoluzione informatica e plasticamente illustrati dall'interazione su internet (si v. § 1.4.3). Si tratta di un fenomeno di straordinaria importanza poiché la novità che contraddistinse il modello di Westfalia rispetto al sistema medioevale delle fonti, consisteva nel passaggio dalla natura personale e fiduciaria delle relazioni giuridiche, basate sullo status degli individui, al criterio territoriale su cui ha fatto leva il modello invalso tra i moderni (§ 4.2.1). Va da sé, questa de-territorializzazione ha tutt'altro significato rispetto all'esperienza medioevale e verrà, come tale, approfondita con la trasformazione che ha condotto dalle consuete frontiere terrestri e marittime degli ordinamenti, agli spazi aerei e satellitari, fino alla dimensione virtuale del cyberspazio.

In terzo luogo, a differenza dei precedenti modelli delle fonti, lo schema di questo paragrafo farà riferimento sia al sistema formale sia, necessariamente, a fonti che allo stato sono ancora *extra*, se non *contra ordinem*. Il motivo dipende non solo dal fatto che, a differenza dei precedenti modelli, siamo alle prese con un sistema in via di perfezionamento e formazione; ma, come riferito fin dall'inizio del presente capitolo, la trasformazione del sistema delle fonti comporta anche, se non soprattutto, questioni di potere. Alla consueta dialettica della separazione dei poteri tra organi del gubernaculum e iurisdictio, va così aggiunta la dinamica, sia spontanea, sia organizzata, dei poteri sociali che, come detto fin dal capitolo primo (§ 1.4.3), si avvale ora della democratica possibilità di scelta tra sistemi diversi, ora, invece, saltando quelli tradizionali, si esprime attraverso nuovi e diversi ordinamenti.

In quarto luogo, nel corso di questo paragrafo, faremo riferimento alle tradizionali idee di gubernaculum, iurisdictio e kosmos, del tutto assenti o quasi nella manualistica, ma non per gusto anacronistico, o come sfida alle convenzioni linguistiche prevalenti al giorno d'oggi. Piuttosto, l'idea è di riassumere con questi concetti, i tre elementi essenziali della dialettica istituzionale contemporanea, ossia il gubernaculum come luogo d'indirizzo politico e legislativo, la iurisdictio come controcanto indispensabile per il controllo delle decisioni del gubernaculum, e il kosmos come dinamica sociale autonoma rispetto alle precedenti sfere. La ragione per cui, a differenza del dualismo di Hayek tra taxis e kosmos (§ 2.2), quest'ultimo è contrapposto a una taxis sdoppiata in gubernaculum e iurisdictio, dipende dalla tensione duale dell'ordinamento, sulla quale si è insistito fin dal capitolo terzo, e al fine di cogliere gli aspetti problematici degli odierni assetti istituzionali relativi alla governance, seguendo l'insegnamento della dottrina costituzionale maturata nel corso degli ultimi otto secoli (§§ 3 e 3.3).

Infine, bisogna avvertire che, per comodità espositiva, lo schema che andiamo a presentare, si limita a fare riferimento alla nozione di kosmos, come già nella tavola 1 del § 4.2.1, senza considerare l'ulteriore distinzione tra consuetudini e autonomia contrattuale delle parti, che sarà esaminata solo nel § 4.3.3.3. L'obiettivo è per ora di sottolineare l'irriducibilità del kosmos rispetto al binomio gubernaculum/iuris-

dictio della taxis, senza appesantire di troppo uno schema che, peraltro, non prende nemmeno in considerazione una delle maggiori novità prodotte dalla rivoluzione tecnologica, vale a dire i temi del design (che, non a caso, saranno l'oggetto di un intero capitolo, il prossimo).

Sulle basi di queste avvertenze preliminari, ecco dunque lo schema che introduce l'analisi delle fonti nelle odierne società ICT-dipendenti:

| Le fonti d'oggi | Diritto Nazionale | Diritto Internazionale | Diritto Transnazionale |
|---|---|---|---|
| Gubernaculum | | | |
| Iurisdictio | | | |
| Kosmos | | | |

Tavola 4: *Le fonti delle società ICT-dipendenti*

La maggiore complessità del modello – 6 osservabili rispetto ai 3 o 4 di quello precedente di Westfalia, 18 potenziali variabili invece di 2 o 3 – dipende dalla necessità di affrontare la maggiore complessità dei fenomeni da descrivere al giorno d'oggi. Naturalmente, non si vuole fornire cifre assolute ma, piuttosto, con gli accorgimenti metodologici introdotti con la tavola 1 in § 4.2.1, si mira a offrire un adeguato livello di astrazione, a metà tra l'intricato reticolo del sistema medioevale delle fonti e la concisa semplicità del modello di Westfalia.

A continuazione, esamineremo il sistema delle fonti, secondo il livello nazionale (§ 4.3.1), internazionale (§ 4.3.2), e transnazionale (§ 4.3.3), e in rapporto alle modalità in cui si danno i fattori produttivi dell'ordinamento. Sebbene questi livelli siano ovviamente intrecciati, la scelta espositiva dipende dal fatto che, in questo modo, emergeranno tanto le differenze, quanto le continuità, che le categorie del gubernaculum, della iurisdictio e del kosmos, rapportate al passaggio occorso dal modello dello stato nazionale sovrano agli odierni assetti della governance, palesano rispetto alla tradizione.

### 4.3.1. *Diritto nazionale*

Si è già avuto modo di segnalare, nelle pagine precedenti, alcuni dei mutamenti occorsi sul piano del diritto nazionale, nel passaggio dal modello di Westfalia all'odierno sistema delle fonti. Per comodità, riassumiamo di nuovo queste trasformazioni.

In primo luogo, si è riferito come uno degli aspetti più rilevanti della rivoluzione tecnologica e con il riposizionamento degli ordinamenti giuridici contemporanei, concerne la crescente inefficacia dell'approccio tradizionale del diritto, inteso come sistema di comandi suffragato dalla minaccia di misure coercitive, "se A, allora B" (si v. § 1.4.3): ciò è soprattutto evidente nel caso della rete di internet.

In secondo luogo, sempre a proposito di gubernaculum, si è visto come in alcuni settori chiave dell'ordinamento, gli stati non dispongano di poteri decisionali e siano anzi stati soppiantati da altri e diversi attori: l'esempio lampante è stato offerto da ICANN e i suoi difficili rapporti con un organismo internazionale come l'ITU (si v. § 3.4.2.1).

In terzo luogo, passando sul piano della iurisdictio, abbiamo detto del suo nuovo ruolo in ambito internazionale: § 4.2.2. Al dualismo costitutivo sul piano interno delle fonti, come insieme d'organi di controllo rispetto a quelli d'indirizzo politico-legislativo, va ad aggiungersi non solo, o non tanto, una rappresentazione dualistica dell'interazione tra diritto nazionale e internazionale, come avviene, ad esempio, con la Consulta italiana e il Tribunale costituzionale tedesco (si v. § 3.2.2). In realtà, come diremo più sotto, è lecito pensare che, soprattutto sul fronte del diritto transnazionale, tale dualismo non potrà che uscire rafforzato dalla crescente complessità del sistema.

Infine, per quanto concerne il kosmos, torna la crescente inefficacia delle misure legislative su internet ma, questa volta, dal punto di vista eguale e contrario degli ordini spontanei di utenti in rete che spesso, semplicemente, ritengono errata la regola stabilita dal legislatore in mala fede o ignorante (si v. § 3.4.3.1).

A queste note si aggiunga inoltre come, alle forme tradizionali d'intervento coercitivo e coattivo, si siano più spesso affiancate forme d'intervento "soffice" che, con la consueta sinteticità dell'inglese, sono chiamate *soft law* (in contrapposizione al *hard law*): all'usuale bagaglio di leggi, codici o accordi internazionali, vanno infatti aggiunti raccomandazioni e opinioni, codici di condotta, linee guida o la standardizzazione delle migliori pratiche in un settore determinato. Come esempio di questo nuovo tipo di fonte, basti menzionare la già ricordata legge 675 che il Parlamento di Roma ha approvato il 31 dicembre 1996, in materia di tutela e protezione dei dati personali: se, nel § 4.1.2, questa legge è servita a chiarire i motivi per cui, anche negli ordinamenti di *civil law*, la giurisprudenza è fonte, qui, invece, la legge serve a chiarire in cosa consistano le fonti soffici [7].

Da un lato, il riferimento va all'istituzione di una nuova figura della iurisdictio, ossia l'"autorità garante" introdotta dall'articolo 28 della direttiva comunitaria in materia di trattamento e protezione dati (D-95/46/CE), puntualmente recepita in Italia con la legge 675. Oltre al controllo sul trattamento dei dati nel rispetto della legge, con l'esame dei reclami, segnalazioni e ricorsi presentati dagli interessati, con l'imposizione di misure affinché il trattamento sia conforme alla legge e con il potere di vietare il trattamento illecito o non corretto, la legge prevede anche funzioni soffici da parte dell'autorità di controllo, come nel caso della segnalazione al governo e al parlamento dell'opportunità di nuovi interventi normativi, anche tenuto conto dell'evoluzione del settore, oltre alla diffusione nell'opinione pubblica di una cultura per i temi della privacy, con la predisposizione annuale di una relazione sullo stato di attuazione della normativa, e via discorrendo. Al pari di quanto avviene con i colleghi su scala europea, come il Gruppo di lavoro articolo 29 (WP 29) o il Ga-

[7] Ad onor del vero, ci sarebbe una terza ragione d'interesse per la legge: infatti, il motivo per cui il Parlamento di Roma l'ha approvata alla vigilia del capodanno 1997 non va ascritto alla solerzia del nostro legislatore; ma, piuttosto, al fatto che l'Unione europea aveva stabilito che entro la data del primo gennaio 1997 gli Stati membri dovevano recepire la direttiva comunitaria in materia di trattamento e tutela dei dati personali (D-95/46/CE), per essere ammessi al "club di Schengen". Si tratta dell'accordo in base al quale i cittadini europei possono liberamente viaggiare in quasi tutti i paesi dell'Unione senza dover esibire il passaporto. Torneremo espressamente su questo punto, a proposito di "trapianti giuridici" (v. § 10.2.2).

rante europeo per la protezione dati, anche l'Autorità garante italiana provvede di qui a stilare una serie di raccomandazioni e opinioni che, pur non supportate dalla minaccia di misure coercitive, finiscono spesso per ottenere il risultato voluto, componendo controversie, anticipando innovazioni legislative, ecc.

D'altra parte, la legge 675, sulla scia comunitaria, ha anche introdotto dei "codici di condotta" che, nei termini dell'articolo 27.1 della disciplina europea, hanno come fine quello di "contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della presente direttiva". Mentre, in Italia, spetta al Garante il compito di promuovere questi codici di autoregolamentazione, avendo poi l'incarico di verificarne la conformità alle leggi e ai regolamenti dell'ordinamento, sono stati nel frattempo approvati il codice per il trattamento dei dati personali nell'esercizio dell'attività giornalistica, quelli per scopi storici, statistici e scientifici, e per i sistemi informativi gestiti dai privati in tema di crediti al consumo, affidabilità e puntualità dei pagamenti.

Come ben si vede, sulla scorta di queste pur succinte annotazioni, si ha a che fare con un modo nuovo di concepire il funzionamento del sistema giuridico tra gubernaculum, iurisdictio e kosmos, che mette in mora un ulteriore pilastro del modello di Westfalia, e cioè a dire l'idea che il diritto consista soltanto in uno strumento di controllo sociale. Si tratta, come detto, di un'idea riconducibile ancora una volta al pensiero di Hobbes e che, nel Novecento, ha trovato tra i suoi massimi esponenti Kelsen. Proprio per la rilevanza del tema, conviene dunque aprire una breve parentesi al riguardo.

#### 4.3.1.1. *Il diritto soffice*

Ci sono tre buoni motivi per soffermarci, in questa sede, sul diritto soffice o *soft law*: sebbene il fenomeno non sia sconosciuto ad altri livelli dell'ordinamento, come il diritto internazionale (v. sin d'ora § 6.3.2), è sul piano del diritto nazionale che la natura autoritativa, più che coattiva, di questa forma di diritto acquista un significato particolare.

Innanzitutto, come suggerito dalla normativa europea in tema di dati personali, che "incoraggia" stati membri e Commissione a promuovere i codici di auto-disciplina, l'interesse per queste forme di diritto soffice risiede nel fatto che il legislatore avvertito e conscio della complessità di ciò che si mira a governare, in fondo delega alla società civile il compito di provvedere al riguardo. Laddove, nelle pagine precedenti, ci si è spesso riferiti al rapporto tra gubernaculum e kosmos nei termini della divaricazione e potenziale conflitto tra le parti in causa, qui, invece, per il tramite di un organo della iurisdictio, il rapporto è di collaborazione.

Secondariamente, le forme del diritto soffice mettono in crisi la distinzione che già Hobbes poneva tra "comando" e "consiglio", al fine di precisare la natura del diritto. Con le parole del capitolo venticinquesimo del *Leviatano*, "si ha comando là dove si dice *Fa' questo* o *Non fare questo*, e non ci si attende nessun'altra ragione che la volontà di colui che lo dice […] Si ha consiglio allorché si dice *Fa' o Non fare questo* non avendo nessun'altra motivazione che il beneficio che ne deriva a colui cui ci si rivolge" (Hobbes ed. 1992: 211). Or bene, le opinioni e raccomandazioni, tra le altre, delle autorità garanti, italiana ed europee, in tema di protezione dati, so-

no tipici esempi di norme non vincolanti che, tuttavia, hanno una forte valenza persuasiva e normativa (Halliday e Osinsky 2006: 449).

Infine, le forme del diritto soffice invitano a riconsiderare la tesi kelseniana del diritto come tecnica del controllo sociale: "se A, allora B". A scanso di equivoci, non si vuole negare il ruolo che le sanzioni e coazioni svolgono nel campo giuridico. Piuttosto, si tratta di comprendere come le regole del diritto non operino in una sorta di vuoto normativo, ma abbiano a che fare con le pratiche sociali di una data comunità; anche non a base territoriale, bensì in rete, come nel caso di internet. Si tratta dell'insegnamento che abbiamo in fondo ricavato, sia pure con le sue contraddizioni, dalla filosofia di Locke (v. § 3.1.1); e, prima ancora, di Socrate, Platone e Aristotele (§§ 1.1 e 1.1.1). Ritraducendo con parole più recenti l'approccio evolutivo al fenomeno giuridico, "strettamente parlando, gli individui non sono costretti a fare ciò che la legge dice loro di dover fare, ma piuttosto ciò che la prevalente convenzione sociale dice che essi sono obbligati a compiere […] Il luogo normativo dell'autorità politica è per ciò la convenzione supportata dalla legge, più che la legge stessa, dato che è la convenzione a risolvere il problema del coordinamento morale, trasmettendo così l'autorità normativa morale alla struttura sociale in questione" (Garthoff 2010: 669 e 680).

### 4.3.2. *Il diritto internazionale*

Abbiamo seguìto nel corso dei paragrafi precedenti, l'evoluzione che ha portato dal vecchio diritto comune europeo, al diritto pubblico europeo, al diritto internazionale classico, fino alla sua ulteriore trasformazione occorsa a metà del secolo scorso, che ha condotto a nuove forme di iurisdictio (§ 4.2.2). A ciò si devono aggiungere le tesi dei globalisti che, in chiave monista, mirano ad allargare la sfera della soggettività internazionale alle organizzazioni non governative e, in fondo, a ogni individuo come cittadino del mondo (§ 3.3.2).

In questa sede, oltre alle istanze cosmopolitiche di Kant, la tesi dei monisti può essere ulteriormente chiarita con l'opera di Kelsen, sotto le vesti di teorico del diritto internazionale, inteso come un unico sistema giuridico su scala planetaria. Rispetto al sistema delle fonti, illustrato in precedenza (§ 4.1), cambia soltanto il disposto della norma fondamentale: al posto del dovere di obbedienza rispetto alla costituzione, la *Grundnorm* del monismo internazionale recita *pacta sunt servanda*, e cioè "bisogna rispettare i patti" (Kelsen ed. 1989).

Tuttavia, abbiamo riferito le ragioni del perché, nonostante le nobili origini, non sia convincente l'approccio dei globalisti: da un lato, pure a tralasciare i problemi pratici del creare un unico costrutto mondiale a base costituzionale, federale e finanche democratica – che tenga assieme Cina, Russia e Stati Uniti d'America – si tratta delle perplessità che suscita il progetto di volere esportare su scala planetaria un approccio, quello monista, entrato in crisi perfino nel suo ambito originale, ossia, quello relativo al gubernaculum degli stati sovrani nazionali nel modello di Westfalia. D'altro canto, sul fronte della iurisdictio, si è detto come il dualismo con cui tradizionalmente le corti decodificano i rapporti tra il proprio diritto nazionale e l'internazionale, sia verosimilmente destinato a rafforzarsi con la crescente complessità del sistema delle fonti, soprattutto sul fronte del diritto transnazionale. Per chia-

rire ulteriormente i termini dell'assunto, vale la pena di tornare a quell'inedita forma di costrutto, nel campo del diritto internazionale, che è l'Unione europea (si v. §§ 3.2.2 e 3.3).

È, infatti, oggetto di un perdurante dibattito che tipo di sistema giuridico possa mai essere quello dell'Unione (si v. Pagallo 2008: 111-112, cui rimando per i riferimenti bibliografici). C'è chi sostiene che si tratti di una sorta di diritto costituzionale "multi-livello", chi di un ordinamento "misto" di elementi democratici e aristo(tecno)cratici, chi di una peculiare versione di federalismo all'europea, chi di una nuova variante del diritto comune medioevale, e chi invece, puntando sulla mancanza della competenza originaria, nota che il modello dell'Unione, dopo tutto, non si allontana poi troppo dalle organizzazioni standard nel campo del diritto internazionale. Questa è sempre stata, in fondo, la tesi del Tribunale costituzionale tedesco, secondo il quale, come si legge ad esempio nella ricordata sentenza sul trattato di Maastricht (si v. § 3.3), "l'assunzione di autorità sovrana da parte di un'Unione di Stati come l'Unione europea è basata sulle autorizzazioni di Stati che rimangono sovrani, agendo nell'ambito internazionale regolarmente tramite i loro Governi e dirigendo così l'integrazione". Ma non basta: siccome "il carattere vincolante del diritto internazionale non può in ogni caso diminuire la protezione dei diritti fondamentali esistente per la Repubblica federale tedesca", non solo "a tale riguardo si applicano le regole che valgono per i trattati internazionali tradizionali". In realtà, aggiunge il tribunale di Karlsruhe, "la necessità di un'attribuzione di competenza stabilita pattiziamente rappresenta da sempre una caratteristica fondamentale dell'ordinamento giuridico della Comunità [oggi Unione]; la competenza dei singoli Stati membri costituisce la regola, quella della Comunità, l'eccezione".

Naturalmente, si dovrebbe ricordare che è proprio questa la tesi condivisa con la Corte di giustizia europea. Ad esempio, si legge nel secondo parere del 2000 emesso dalla Corte di Lussemburgo ai sensi dell'allora vigente articolo 300(6) del trattato sull'Unione, "la scelta della base giuridica appropriata ha rilevanza costituzionale. Dal momento che la Comunità ha soltanto poteri conferiti, essa è legata alla previsione del Trattato che le conferisce detti poteri onde approvare una data misura", per cui "procedere in ragione di una incorretta base legale è per ciò passibile di portare all'invalidazione dell'atto con il quale è stato concluso un accordo, viziando in questo modo il consenso che lega la Comunità all'accordo sottoscritto da essa" (§ 5 dell'Opinione). Quale, dunque, la ragione del dissidio tra le corti?

Per certi versi, la risposta va ricercata in senso eguale e contrario al diritto soffice tratteggiato nel paragrafo precedente, vale a dire nel *hard law*, piuttosto che nel *soft law*. Sebbene, infatti, nel corso degli ultimi decenni, sia prevalso fortunatamente un certo pragmatismo e finanche uno spirito di collaborazione tra le corti, è un dato di fatto che torni ciclicamente la domanda: insomma, chi è il "custode dei trattati" (v. § 3.2.1)?

### 4.3.2.1. *L'Unione europea tra monismo e dualismo*

Fin dal trattato istitutivo del 1957, con l'allora articolo 177, poi divenuto 234 e, oggi, 267 del TFUE (Trattato sul funzionamento dell'UE), la risposta alla domanda su chi sia mai "il custode dei trattati" è che questi non è altri che la Corte di Lus-

semburgo "competente a pronunciarsi in via pregiudiziale" sulla loro interpretazione. Da questo primo punto di vista, sembra doversi pertanto avvallare la lettura monista della Corte di giustizia, ossia l'approccio, già caro a Kelsen, per cui l'interazione tra diritto degli stati membri e diritto europeo può essere concepita come integrata in un unico sistema. Questa conclusione, non senza una certa dose di paradosso, sembra peraltro confermata proprio dalle "regole che valgono per i trattati internazionali tradizionali", per dirla con il Tribunale costituzionale tedesco, nel senso che, come visto in precedenza (§ 1.2.1), a proposito del caso che oppose il Canada alla Francia su come interpretare le clausole dell'articolo XX (b) del GATT, sono stati in definitiva il Panel del WTO in primo grado e, quindi, l'organo d'appello della stessa organizzazione mondiale sul commercio ad avere avuto l'ultima parola nella controversia.

Tuttavia, nel caso dell'UE, c'è una fondamentale differenza che separa il costrutto dalle altre organizzazioni internazionali: come detto (§§ 3.2.2 e 3.3), non si tratta soltanto delle più estese competenze di cui gode l'UE, ma del fatto che molte sue disposizioni vincolano direttamente gli stati membri, così come i loro cittadini. Da questo ulteriore punto di vista, si può cioè dire che, nella propria sfera di competenza, l'Unione funzioni come uno stato federale, in quanto il tipico filtro della ricezione del diritto internazionale tramite un'apposita disposizione del diritto interno viene meno. Infatti:

a) sulla base della legittimità costituzionale definita dai trattati, i legislatori dell'UE, vale a dire Consiglio e Parlamento, esercitano congiuntamente detta funzione, approvandone i regolamenti e le direttive;

b) gli stati membri provvedono, se del caso, a recepire tali atti nei propri ordinamenti e, però, nel caso di contrasto tra normativa dello stato membro e normativa UE, prevale sempre quest'ultima;

c) tale supremazia comporta che i giudici nazionali siano tenuti a disapplicare il proprio diritto nel suddetto caso di contrasto, decidendo delle controversie direttamente sulla base del diritto europeo unitario;

d) in caso di dubbi, si ricorre al rinvio pregiudiziale dell'articolo 267 di cui sopra.

Questo funzionamento quasi-federale dell'Unione, sul quale dovremo tornare più tardi, a proposito della normativa europea in tema di trattamento e protezione dei dati, non può che incidere sul riposizionamento del diritto nazionale esaminato poc'anzi (in § 4.3.1). Basti pensare alla situazione, per molti versi clamorosa, verificatasi in Germania con il caso di Tanja Kreil e del suo desiderio di ottenere un impiego militare comportante l'uso delle armi; desiderio che, tuttavia, la Costituzione federale tedesca del 1949 escludeva in linea di principio. La lite, cominciata a proposito del principio di parità di trattamento tra uomini e donne nell'accedere ai posti di lavoro, sarebbe arrivata nel 1998 davanti alla Corte di giustizia, smettendo ben presto di essere una mera questione economica e di salvaguardia del mercato unico, secondo il tenore della direttiva 76/207/CEE, per chiamare in causa il principio di eguaglianza tra i sessi come diritto fondamentale della persona. Innanzi alla decisione della Corte di Lussemburgo, l'11 gennaio 2000, sulla base della direttiva che "osta all'applicazione di norme nazionali, come quelle del diritto tedesco, che esclu-

dono in generale le donne dagli impieghi militari comportanti l'uso delle armi" (C-285/98), il risultato è stato che la Repubblica federale tedesca si è vista costretta a modificare il 19 dicembre 2000 la Costituzione, emendandone l'articolo 12a(4) per violazione dei diritti fondamentali posti alla base dell'allora diritto comunitario.

A conferma delle difficoltà cui vanno a parare gli approcci dualistici al diritto europeo, per cui, come afferma ad esempio la Consulta italiana nel caso Granital (si v. § 3.2.2), si tratta di due ordinamenti "separati e distinti ancorché coordinati", potremmo aggiungere gli effetti indesiderati di una discriminazione alla rovescia. In sostanza, in nome del mercato unico e della libera concorrenza, la normativa europea ha consentito a imprese "straniere" di produrre birra in Germania, formaggi in Francia o pasta in Italia, secondo standard, per l'appunto, europei e non più solo nazionali (nel bene e nel male). A inquadrare lo scenario con un'ottica dualistica, la conseguenza è stata che, spesso, i produttori locali si sono ritrovati sfavoriti dalla normativa del proprio stato d'origine rispetto alla concorrenza straniera, tenuta a rispettare i soli standard comunitari. Davanti all'interrogativo sollevato nel caso della "disciplina per la lavorazione e commercio dei cereali, degli sfarinati, del pane e delle paste alimentari" di cui alla legge 580 del 1967, in rapporto alla parità di trattamento sancita dal terzo articolo della Costituzione italiana, l'effetto indesiderato è stato che, adottando una prospettiva internazionalistica di stampo dualistico, come quella della Consulta di Roma, risulta poi difficile pronunciarsi sulla legittimità delle leggi approvate dal Parlamento italiano, in rapporto a parametri di una normativa, quella europea, considerata a tutti gli effetti sempre e solo "straniera".

A complicare le cose, bisogna però ammettere che l'ordinamento europeo, se pure funziona sotto certi aspetti come un sistema federale, non è, né è detto lo sarà mai, un ordinamento di tale tipo. A ciò osta, come ama ripetere il Tribunale costituzionale tedesco, la competenza originaria che fa capo agli stati membri e il fatto che una serie di settori cruciali dell'ordinamento, ora, come nel caso del diritto penale e molte parti del civile, come il diritto di famiglia, sono ancora nelle mani degli stati sovrani; ora, come nel caso della politica estera e di sicurezza comune, sono sottratti ai poteri giurisdizionali della Corte di giustizia (art. 275 TFUE); ora, come nel caso della tutela dei diritti umani, sono devoluti in ultima istanza a un ulteriore organo di diritto internazionale come la Corte europea dei diritti dell'uomo con sede a Strasburgo; ora, come nel caso della difesa militare, a un'alleanza come la NATO.

Su queste basi, è dunque forse comprensibile che le corti costituzionali nazionali esitino ad abbracciare senza riserve il monismo della Corte di giustizia e, ciò, nonostante il fatto che il loro opposto dualismo suggerisca tetri paragoni con passate esperienze federali. Si tenga infatti presente che la ragione formale per la quale ebbe inizio la guerra civile nordamericana, nel 1861, fu il rifiuto che gli Stati del Sud opposero alla decisione della Corte suprema di Washington in materia di schiavitù, e che parte degli studiosi ritenga che si possa parlare degli Stati Uniti d'America come di un vero e proprio stato federale solo dopo che quella guerra civile venne conclusa con la vittoria degli Stati del Nord nel 1865 (Lombardi 1987). Del resto, non è certo questa la prima volta che la nostra analisi va a parare in guerre civili e rivoluzioni, a loro volta annoverabili tra le fonti *contra ordinem* del diritto: si v. § 4.1.1 con rimando alle tesi di Hobbes (§ 2.1.2.1), e di Locke (§ 3.1.1). Che, poi, l'analisi sulle fonti *contra ordinem* s'intrecci con le interpretazioni sul sistema legale delle fonti è

comprensibile perché, come detto, le redistribuzioni sul piano delle fonti vanno di pari passo con questioni di potere. Così, nel caso della rivoluzione inglese, si è visto come il conflitto si sia aperto tra chi, Re, rivendicava la lettera e chi, Corti e Parlamento, s'appellava allo spirito delle istituzioni monarchiche inglesi (§ 3). Nel caso della rivoluzione americana, tra chi, Patrioti, faceva inizialmente leva sulle carte coloniali e chi, Parlamento inglese, sul nuovo assetto istituzionale uscito dopo la rivoluzione di quel paese (§ 3.1.3.1). Nel caso dell'Unione europea, sia pure con i debiti scongiuri, il contrasto è tra chi, come la Corte di Lussemburgo, insiste sulla lettera dell'articolo 267 TFUE e chi, come il Tribunale costituzionale tedesco o la Consulta italiana oppone, in chiave dualistica, la propria competenza. Con le parole impiegate dalla Consulta il 27 dicembre 1973, ancora perno indiscusso della sua giurisprudenza, le tesi della Corte di Lussemburgo non possono mai "comportare per gli organi della CEE [oggi UE] un inammissibile potere di violare i principi fondamentali del nostro ordinamento costituzionale o i diritti inalienabili della persona umana. Ed è ovvio che qualora dovesse mai darsi all'art. 189 Trattato CEE una sì aberrante interpretazione, in tale ipotesi sarebbe sempre assicurata la garanzia del sindacato giurisdizionale di questa Corte sulla perdurante compatibilità del Trattato con i predetti principi fondamentali" (sentenza 183 sulla legittimità costituzionale dell'articolo 2 della legge 1203 del 14 ottobre 1957, che ha reso esecutivo in Italia il trattato CEE).

Da allora, come detto, è venuto prevalendo un sano pragmatismo tra le corti che il 7 febbraio 2014 ha condotto, tra le altre cose, al primo rinvio alla Corte di Giustizia da parte del Tribunale costituzionale tedesco, sulle misure prese nel settembre 2012 da parte della Banca centrale europea al fine di rafforzare o, finanche, salvare l'euro. Si tratta di un processo che va accolto con estremo favore poiché, in fin dei conti, è proprio il processo d'integrazione europea ad aver rappresentato uno dei principali motivi per cui i consueti scenari di guerra che hanno scandito la storia d'Europa per secoli, sono diventati irreali nel corso delle ultime due generazioni. La pace nel vecchio continente, in altri termini, è indissolubilmente legata alle sorti del processo d'integrazione europea e al modo in cui ne concepiamo le fonti.

Ma, proprio le insuperabili difficoltà cui si va incontro nell'inquadrare l'odierno stato dell'Unione, nella contrapposizione tra monismo e dualismo tipica del diritto internazionale, consigliano di tornare allo schema dal quale siamo partiti, ossia la tavola 4 del § 4.3. Nelle discussioni che affaticano la dottrina a proposito di conflitti internazionali tra giurisdizioni e limiti quasi-federali alla sovranità degli stati membri, ritroviamo infatti la preoccupazione dei "globalisti" sul piano del diritto internazionale, nella loro polemica con le tesi dei "realisti". Cerchiamo a continuazione di spiegarne il perché.

### 4.3.2.2. *Il terzo assente*

Abbiamo ricordato nelle pagine relative ai livelli della governance (§ 3.3.2), la tesi di Bobbio per cui è l'assenza di un "Terzo superiore alle parti" che spiega la condizione di disordine in cui versa il diritto internazionale. Si tratta di un approccio monista fondato sul consenso e sul controllo delle parti di cui il Terzo deve dirimere il conflitto che, in sostanza, proietta nel campo del diritto internazionale le categorie a noi ben note sul piano del diritto interno.

Tuttavia, sia in rapporto ai dilemmi odierni dell'Unione europea, stretta tra monismo e dualismo, sia delle istanze dei "globalisti" su scala internazionale, la tesi sul "terzo assente" acquista, in questo contesto, tutt'altro significato. Alla luce dei problemi di gubernaculum e iurisdictio che siamo venuti fin qui discutendo, l'assenza del terzo suggerisce perché il ruolo del kosmos non sia stato preso in considerazione: infatti, quale ruolo potremmo mai affidare alla formazione degli ordini spontanei se, appunto, gli attuali dilemmi tra monismo e dualismo rimandano al contrario a un contrasto mai sopito?

Il punto può essere illustrato, aggiornando la tavola 4 del § 4.3, con un nuovo schema:

| Le fonti d'oggi | Diritto Nazionale | Diritto Internazionale | Diritto Transnazionale |
|---|---|---|---|
| Gubernaculum | | | |
| Iurisdictio | | | |
| Kosmos | | ? | |

Tavola 5: *L'assenza del terzo*

La figura del kosmos come terzo assente getta luce sul modo tradizionale di concepire le categorie del diritto internazionale classico e, per questa via, il vicolo cieco in cui è andato a parare il dibattito odierno tra i cultori del diritto europeo e la polemica tra le corti a livello internazionale. Si tenga presente che, nella sua accezione originaria, alla lettera, il diritto internazionale era il diritto, appunto, "tra" (*inter*) nazioni, per cui, come più volte accennato in riferimento ai pilastri del modello di Westfalia, gli unici soggetti di questo settore del diritto erano gli stati nazionali sovrani. Solo in un secondo momento (§ 4.2.2), sono entrati in campo gli organi della iurisdictio, per cui un'ulteriore caratteristica del nuovo costrutto europeo, a proposito dei quattro principi cardini della libera circolazione delle persone, delle merci, dei servizi e dei capitali, come tali attinenti alla sfera del kosmos, ha riguardato il criterio dell'"applicabilità diretta" o "immediata" del trattato istitutivo del 1957 (§ 3.2.2). Questo impianto sarebbe stato in séguito coronato dagli accordi di Schengen (1985), e dal trattato di Maastricht (1993) che, istituendo la figura della cittadinanza europea, stabiliva il diritto di circolazione e soggiorno in tutto il territorio dell'Unione.

Dopo il successivo trattato di Amsterdam (1999), sarebbe iniziata la fase relativa a un trattato costituzionale europeo approdato, poi, nel nulla, sia per l'insipienza teorica dei sedicenti padri costituenti, sia per l'oggettiva difficoltà del compito. A differenza, infatti, dei padri fondatori statunitensi, non soltanto mancava qualcosa di analogo a un "we the people" in chiave europea (v. § 3.1.3.1 (i)); ma, fatto questo ancor più devastante, alcuni popoli europei, dopo l'entrata in vigore del trattato di Nizza (2003) e la firma a Roma del nuovo trattato che avrebbe adottato una Costituzione per l'Europa (2004), respingevano quest'ultimo accordo con due referendum: quello dei cittadini francesi il 29 maggio 2005 e quello dei Paesi Bassi il primo giugno di quello stesso anno. Sebbene parti degli accordi sarebbero state trasfuse nel successivo trattato (2007), quello di Lisbona (2009), dal punto di vista sostanzia-

le, che è poi quello che qui preme rimarcare, i termini del vicolo cieco sarebbero rimasti inalterati:

– o come afferma il Tribunale costituzionale tedesco, l'Unione europea si basa sulle autorizzazioni di stati che rimangono sovrani e, come tali, agiscono nell'ambito internazionale regolarmente tramite i loro governi; ma, allora, con le categorie del diritto internazionale, tra gubernaculum e iurisdictio, non c'è spazio per alcun kosmos;

– oppure, come ritiene la Corte di giustizia, bisogna adottare un approccio monista per cogliere la novità dell'integrazione europea; nel qual caso, però, il problema consiste nella difficoltà palesata dalle sue istituzioni d'intercettare (ed entrare in contatto con) le dinamiche del kosmos, nel modo che abbiamo cominciato a osservare sul piano del diritto nazionale.

Quest'ultima difficoltà, d'altra parte, riconduce all'altro dilemma dei "globalisti" e "realisti" sul fronte del diritto internazionale. Per i primi, si tratta di ampliare la sfera della soggettività politica del diritto internazionale, fino a includervi ogni individuo concepito come cittadino del mondo. Da questo punto di vista, l'accento cade necessariamente sul piano della progettualità del costruttivismo giuridico, dato che, appunto, occorre mettere mano ai meccanismi e istituti tradizionali del diritto internazionale. Tuttavia, per quanto lodevole e condivisibile possa essere l'intento, non solo rimangono i dubbi e perplessità già sollevati sia sul piano della realizzabilità del progetto, sia sul suo impianto monista (si v. § 4.3.2). In realtà, ciò che rimane assente è il ruolo che gli ordini spontanei del kosmos possono mai svolgere all'interno di questa teoria: come detto nelle pagine sul diritto nazionale (si v. § 4.3.1.1), bisogna insistere sul fatto che le norme giuridiche non operano in una sorta di vuoto, ma hanno a che fare con dinamiche e pratiche sociali che occorre, appunto, istituzionalizzare.

Infine, ma non da ultimo, proprio queste dinamiche e pratiche sociali sono state esaminate dai teorici del realismo nel diritto internazionale: si v. § 3.3.2. Eppure, l'angolo prospettico per lo più adottato dai realisti ha finito per condizionarne l'analisi, nel senso che l'ambito entro cui collocare il ruolo svolto dai processi d'ordine spontaneo non va tanto ricercato oggi nel campo del diritto internazionale; ma, in quel nuovo settore dell'ordinamento che, più spesso, a partire dalla seconda metà del secolo scorso, è detto diritto transnazionale. È dunque a quest'ultimo diritto che è dedicata la parte conclusiva del capitolo.

### 4.3.3. *Il diritto transnazionale*

Dopo il diritto nazionale e quello internazionale, la terza serie d'osservabili del sistema delle fonti relativo alle società ICT-dipendenti concerne il diritto transnazionale. Tra i primi, o come prima definizione del concetto, dobbiamo risalire alla serie di lezioni tenute a Yale, nel 1956, da Philip Jessup (1897-1986), secondo cui la nozione di diritto transnazionale avrebbe dovuto "includere tutto il diritto che regola azioni o eventi che trascendono le frontiere nazionali. Sono inclusi tanto il diritto internazionale pubblico che privato, così come le altre regole cui non si attagliano pienamente siffatte categorie tradizionali" (Jessup 1956: 2).

La data in cui Jessup comincia a delineare la nuova e fortunata nozione, 1956, non è certo casuale: secondo la nostra periodizzazione (§ 4.2.3), inizia ad apparire sempre più evidente la crisi del precedente sistema delle fonti, sintetizzato come modello di Westfalia, con la concomitante difficoltà, da un lato, di riassumere le fonti del diritto con la tradizionale coppia di diritto nazionale e diritto internazionale; d'altro canto, con la necessità di dar conto del ritorno delle norme sociali e la *lex mercatoria* tra le fonti del sistema giuridico.

Uno dei problemi posti dalla definizione di Jessup, tuttavia, era – e per certi versi rimane ancora – posto dal come intendere le "altre regole" cui il giurista nordamericano faceva riferimento. Si tratta di una difficoltà che tuttora divide gli studiosi quando devono precisare il significato del termine, per tre ragioni principali: innanzitutto, si può pensare al termine di diritto transnazionale, declinando quel "trans" ora come ciò che va oltre, ma ingloba pur sempre, il diritto nazionale; ora, invece, per indicare un diritto globale "senza lo stato" (Teubner 2007).

In secondo luogo, la difficoltà di individuare un'univoca accezione del termine dipende dal fatto che esso è più spesso riferito a una pluralità di settori eterogenei: così, si parla di diritto transnazionale a proposito delle "altre regole" relative ai regimi giuridici interni delle società multinazionali e la *lex mercatoria*, alle imprese e sindacati come attori privati del diritto internazionale del lavoro, al diritto transnazionale dello sport o ai diritti umani (Zumbansen 2006); oltre, va da sé, il settore di internet.

Infine, si ricorre al termine transnazionale in chiave negazionista, ossia per negare che i fenomeni che attraversano le tradizionali frontiere giuridiche e politiche degli stati richiedano una disciplina diversa da quella tradizionale. Ad esempio, nel caso di internet, si è affermato che il suo impatto transnazionale sugli ordinamenti andrebbe concepito "identico all'attività transnazionale mediata da altri mezzi, come la posta o il telefono o i segnali di fumo" (Goldsmith 1998: 1239-40).

Come già nel capitolo primo, a proposito delle tesi del tecno-determinismo (§ 1.2), l'indagine muoverà dall'ultimo punto sollevato dai negazionisti: se avessero infatti ragione questi ultimi, non ci sarebbe motivo di procedere oltre con l'analisi di un diritto inesistente o inutile! Siccome, però, vedremo che questo non è proprio il caso, l'indagine proseguirà, mettendo in luce le peculiarità del diritto transnazionale, ora, come diritto "oltre" lo stato (§ 4.3.3.2); ora, invece, come diritto globale "senza" lo stato (§ 4.3.3.3).

#### 4.3.3.1. *Le tesi del negazionismo*

Alcuni autori contestano la necessità di ricorrere alla nuova nozione del diritto transnazionale perché, in buona sostanza, le categorie consuete del diritto nazionale e del diritto internazionale sarebbero in grado di disciplinare opportunamente eventi o azioni a carattere transnazionale. Così, si sostiene che "in assenza di soluzioni internazionali consensuali, i prevalenti concetti di sovranità territoriale consentono a una nazione di regolare gli effetti locali di condotte extraterritoriali" (Goldsmith 1998: 1212). In fondo, si tratterebbe dei consueti criteri con cui, da secoli, gli ordinamenti risolvono questioni di competenza e giurisdizione nel diritto internazionale privato e pubblico. Basti pensare a tecniche come quelle di stabilire la presenza di persone o cose su un dato territorio, come condizione di applicabilità della norma-

tiva nazionale; oppure, di specificare tramite una lista di stati a quali di essi si applichi, o meno, la legge; oltre al principio di finalità territoriale della legge per calibrarne selettivamente l'applicabilità; oppure, al principio di reciprocità tra i sistemi, e via di questo passo.

Come esempio di questi criteri valga uno che tornerà poi utile nel prosieguo della riflessione, ovvero l'articolo 4 della ricordata direttiva europea in tema di trattamento e protezione dei dati personali D-95/46/CE (§ 4.3.1). Al fine di stabilire quando un diritto nazionale è applicabile, il legislatore di Bruxelles punta su:

a) le attività che uno stabilimento del responsabile del trattamento svolge nel territorio di uno stato membro, a meno che esso si ritrovi in più stati; nel qual caso, il responsabile deve garantire che ciascuno dei suoi stabilimenti segua gli obblighi stabiliti da ciascun diritto nazionale applicabile;

b) il diritto internazionale pubblico che disciplina l'attività del responsabile che non sia stabilito nel territorio dello stato membro, ma in un luogo in cui si applica la sua legislazione nazionale;

c) il ricorso, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di uno stato membro, da parte di un responsabile del trattamento che non sia stabilito nel territorio dell'Unione.

Al pari degli altri criteri con cui tradizionalmente si è inteso risolvere i conflitti di competenza e giurisdizione sul piano internazionale, tuttavia, anche quelli dell'articolo 4 presentano un problema. Tali criteri sono stati infatti concepiti in un mondo, nel quale la regola era data dal radicamento delle cose e delle persone in un ordinamento giuridico, mentre l'eccezione era rappresentata dalla necessità di regolare gli effetti locali delle condotte extra-territoriali in quel dato ordinamento. In un mondo in cui tale rapporto si rovescia, tali criteri conducono a esiti paradossali perché, come ripetutamente segnalato nelle pagine precedenti (§§ 2.2.2 e 3.1.3.1 (iv)), la scala o dimensione dei problemi conta!

Da un lato, l'applicazione di criteri, come quelli dell'articolo 4, possono portare a collidere con uno dei corollari del principio democratico (v. § 3.1.2), dato che individui che non hanno preso parte alla normativa in questione, sia per via diretta o indiretta, finiscono tuttavia per esserne assoggettati. Basti pensare a ciò che le Autorità garanti europee nel campo della protezione dati sono venute affermando fin dalla loro Opinione del 2002 (doc. WP 56), per cui, al fine di tutelare i diritti dei cittadini europei nei confronti di società, spesso nordamericane, che trattano dati oltre i confini dell'Unione, come capita con Google, Facebook o Twitter, i "cookie" dovrebbero essere concepiti come strumenti ai sensi della lettera (c) dell'articolo 4. Il risultato di questa particolare interpretazione dei cookie[8], sarebbe stato che ogni qualvolta un cittadino cinese o indiano si fosse recato in vacanza, poniamo, a Capri, e di lì, poi, avesse cominciato a controllare i suoi conti online presso la banca nazionale, la normativa di riferimento, a rigore, avrebbe dovuto essere quella europea!

[8] I cookie sono file, o stringhe di testo, immesse nei computer degli utenti in rete, che servono all'autenticazione automatica, alla tracciatura delle sessioni o a memorizzare alcune informazioni specifiche degli utenti stessi, per agevolare idealmente i servizi dei siti web, una volta che gli utenti vi facciano ritorno.

D'altro canto, non sorprenderà che questo approccio risulti spesso inefficace, al punto da aver costretto molti stati nazionali, come anche l'Unione europea, a scegliere criteri più selettivi, sulla cui base, poi, mirare a far valere le proprie leggi. Questo è, per esempio, il caso del regolamento europeo 44 del 2001, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni relative a contratti in materia civile e commerciale, che, all'articolo 15.1(c), attrae nella competenza di uno stato membro le attività commerciali e professionali di persone al di fuori dell'Unione, ma che siano "dirette, con qualsiasi mezzo, verso tale Stato membro [e] purché il contratto rientri nell'ambito di tale attività". Simile criterio è del pari impiegato nel Regno Unito, dove le corti hanno stabilito che, nel caso di dispute sulla violazione della legge britannica in materia di segni distintivi, l'uso di questi ultimi su internet rileva ai fini dell'ordinamento, soltanto se l'attività del sito web è "diretta" ai consumatori britannici (Reed 2012: 42). Sebbene altri autori abbiano notato come, per quanto si restringa in questo modo la sfera di competenza giurisdizionale degli stati, la certezza del diritto rimane per lo più illusoria (Hörnle 2009), basti notare la duplice difficoltà in cui vanno inevitabilmente ad arenarsi le tesi di chi abbiamo qui definito "negazionisti".

La prima difficoltà riguarda ciò su cui si è insistito in questo paragrafo, per via dell'intento di applicare alle società ICT-dipendenti criteri normativi appartenenti a un mondo che, per molti versi, semplicemente non c'è più. Il risultato è l'inefficacia cui va spesso incontro l'approccio tradizionale alle questioni di giurisdizione e competenza nelle società ICT-dipendenti.

La seconda difficoltà concerne invece il fatto che, nonostante i problemi di attuazione delle norme da parte dei sistemi giuridici nazionali, il risultato non è caos, bensì kosmos. L'assenza o inefficacia dell'intervento dello stato non conduce a una nuova sorta di stato di natura al modo di Hobbes (§ 2.1.2.1); ma, piuttosto, si ha a che fare con nuove forme di ordinamento delle relazioni sociali, che spesso sono riassunte, appunto, con la formula del diritto transnazionale. Esaminiamo più da vicino questi tipi di kosmos contemporaneo.

### 4.3.3.2. *Oltre lo stato*

Abbiamo cominciato a vedere nel corso delle pagine precedenti, sia esempi di kosmos odierno sia di diritto "oltre lo stato".

Nei §§ 1.4.3 e 3, il riferimento è andato agli utenti che preferiscono seguire le consuetudini e usi della rete, piuttosto che le regole di un legislatore lontano, secondo un fenomeno peraltro ampiamente studiato in dottrina.

Nel § 3.4.2.1, ci si è soffermati sulla figura d'ICANN e le sue competenze per garantire un unico dominio di nomi e numerazione in internet, laddove il ruolo degli stati, sebbene molte delle decisioni possano avere alta incidenza politica, economica e sociale, è limitato a una mera funzione consultiva.

A questo punto, possiamo approfondire la nostra indagine sui profili inerenti al diritto transnazionale contemporaneo, alla luce di un nuovo esempio noto a molti lettori, trattandosi del popolare sito americano di compravendite e aste online, "eBay".

Le regole che definiscono l'interazione tra gli utenti sono stabilite dalla stessa

eBay con un insieme di obbligazioni contrattuali che, nel corso degli anni e con la crescita esponenziale del sistema, ha man mano tenuto conto dei commenti, delle opinioni e delle aspettative degli utenti (Goldsmith e Wu 2006: 130-145). Il riferimento va ai principi di trasparenza, buona fede e correttezza, che si cristallizzano con un punteggio relativo alla reputazione di ciascun venditore e compratore che si avvale della piattaforma del sistema. I diritti degli utenti sono tuttavia, per molti versi, attenuati rispetto a determinate legislazioni nazionali, o come nel caso della normativa europea per la protezione e tutela dei consumatori: gli utenti hanno infatti diritto a essere rimborsati solo se hanno fatto uso del meccanismo di pagamento PayPal, acquistato nel 2002 da eBay, e soltanto a condizione che ciò che si è comprato non sia mai stato recapitato o non corrisponda a quanto detto dal venditore (nel qual caso, eBay è sempre in grado di annullare la transazione di pagamento tramite PayPal).

Nonostante questi accorgimenti, non sono mancate ovviamente le liti: in linea teorica, essendo rapporti fondati su contratti, si potrebbe pensare che la fonte ultima del sistema per dirimerne le controversie, sia la normativa nazionale degli utenti interessati. In fondo, trattandosi dei servizi che eBay rende agli utenti tramite la sua piattaforma, non sono nemmeno mancate cause intentate contro eBay: basti far cenno alla lite, iniziata dalla ditta francese l'Oréal nei confronti di eBay per la rivendita non autorizzata e la contraffazione di prodotti con il marchio della nota casa francese sulla piattaforma della società californiana (nella causa 324/2009, decisa dalla Corte di giustizia di Lussemburgo il 12 luglio 2011, con sostanziale vittoria per l'attore).

Ma, all'atto pratico, capiremmo poco di come funzionino gli ordinamenti giuridici contemporanei se ci fermassimo a questo, sia pure, fondamentale aspetto. Nella maggior parte dei casi, infatti, le controversie tra gli utenti di eBay non finiscono davanti alle corti degli stati nazionali, vuoi per il valore economico delle liti, che sconsiglia il più delle volte il ricorso a quelle corti, vuoi per la natura delle controversie che hanno a che fare con individui che spesso risiedono in luoghi diversi del pianeta, vuoi per l'efficienza del sistema legale di eBay che deve, in ogni caso, mantenere la fiducia dei propri utenti, se vuole continuare a fare affari (Schultz 2007).

Inoltre, vale a maggior ragione per gli ordinamenti transnazionali come quelli di eBay, quanto detto a proposito del diritto nazionale, cioè a dire che essi non operano in una sorta di vuoto normativo, ma rimandano alle pratiche sociali e ai valori di una data comunità (§ 4.3.1.1). L'autorità di cui godono questi ordinamenti transnazionali, infatti, non dipende né da un presunto contratto sociale (§§ 3.1.1 e 3.1.2), né dal postulato di una norma fondamentale (§ 4.1). Piuttosto, questi ordinamenti traggono la propria autorità "dall'accordo della comunità che quelle regole siano appropriate a disciplinare le loro transazioni. Come risultato, coloro i quali scelgono di diventare membri della comunità in questione, sottomettono se stessi, attraverso la loro scelta, all'autorità delle regole transnazionali che governano la comunità" (Reed 2012: 89). Si tratta di un meccanismo che, a detta di numerosi autori, è anche all'opera con le norme dell'odierna *lex mercatoria*, per cui la forza normativa delle odierne norme del diritto transnazionale commerciale dipenderebbe dalla sottomissione volontaria dei partecipanti a questo sistema di regole: "per esempio, se una persona accetta il ruolo o l'identità di commerciante, ne consegue che si appliche-

ranno le norme della *lex mercatoria* che rilevano per quel dato gruppo di commercianti" (Linarelli 2009: 196).

Su queste basi, occorre fare ritorno alla tavola 4 introdotta nel § 4.3, per integrarla di conseguenza. Bisogna distinguere, all'interno del kosmos, tra contratti e consuetudini, nello stesso modo in cui la taxis è stata scomposta sin dal capitolo terzo in gubernaculum e iurisdictio, per dar conto della complessità dei fenomeni osservati. Come illustra il caso della *lex mercatoria*, abbiamo a che fare ora con la forza vincolante degli accordi intrapresi dalle parti, ora con norme consuetudinarie relative alla procedura, prove e testimonianze, ora con i principi generali del diritto commerciale. Questa differenziazione trova del resto conferma nella pletora di comunità online, come nel caso di eBay, perché l'insieme delle regole con cui i membri di quelle comunità interagiscono, non va confuso con gli accordi che discendono dai loro eventuali contratti. Il risultato è che le fonti delle odierne società ICT-dipendenti vanno indagate alla luce di 7 (e non solo 6) osservabili, come illustrato dallo schema seguente:

| Le fonti d'oggi | Diritto Nazionale | Diritto Internazionale | Diritto Transnazionale |
|---|---|---|---|
| Gubernaculum | | | |
| Iurisdictio | | | |
| Contratti | | | |
| Consuetudini | | | |

Tavola 6: *Il sistema complessivo delle fonti nelle società ICT-dipendenti*

Indubbiamente, rispetto allo schema della tavola 4, quello della tavola 6 è più complesso: con le indicazioni metodologiche del § 4.2.1, passiamo da 18 a 30 possibili variabili del sistema.

L'accresciuta complessità dello schema, nondimeno, si giustifica in ragione di tre punti principali: in primo luogo, l'irriducibilità dei contratti rispetto alle leggi, o agli usi e consuetudini, mette in chiaro la tesi di molti nell'ambito del diritto transnazionale, e cioè il ruolo vitale che i contratti svolgono, ad esempio, nella governance di internet (Bygrave 2012).

In secondo luogo, il fatto che i contratti consentano in linea di principio una gestione più flessibile degli ambienti digitali, getta a sua volta luce sul ruolo dei contratti nel campo del diritto nazionale. Un esempio classico è dato dall'autonomia contrattuale delle parti nell'ambito del diritto sindacale, oltre al dibattito mai sopito tra giuspositivisti e giusnaturalisti, circa il valore del contratto come legge tra le parti.

Infine, distinguendo tra contratti e consuetudini come osservabili irriducibili del kosmos, siamo in grado di approfondire il tema del "terzo assente" emerso con il diritto internazionale (§ 4.3.2.2). Da un lato, è pacifico che si diano in quest'ultimo ambito dei contratti e che la consuetudine, a sua volta, rappresenti una fonte tradizionale dei rapporti "tra" (*inter*) nazioni. D'altro canto, l'assenza del terzo lamentata nelle pagine precedenti, suggerisce però che la dinamica relativa alla formazione d'ordini spontanei vada intesa alla luce del diritto transnazionale, più che interna-

zionale, in rapporto alle modalità secondo cui si formano le comunità. Se, nei §§ 2.2.2 e 2.2.2.1, si è insistito su alcune delle leggi secondo cui gli ordini emergono spontaneamente dalla complessità dell'interazione sociale, in questo paragrafo l'accento è caduto sull'intesa tra le parti di accordarsi sulle regole ritenute appropriate a disciplinare le loro interazioni. Ciò che è tuttavia rimasto, allo stato, ancora controverso, è come raccordare questa autonomia privata delle parti alla tradizionale organizzazione nazionale e internazionale dei poteri pubblici. Dopo la prima accezione del diritto transnazionale come diritto "oltre" agli stati, bisogna appurare se, e in quale misura, si tratti piuttosto di un diritto "senza" i medesimi.

#### 4.3.3.3. *Senza o contro lo stato?*

Abbiamo segnalato in precedenza (§ 2.1.2.2), come la crescente complessità dei sistemi sociali sia andata di pari passo con la moltiplicazione dei centri di produzione normativa. Tornando alle parole di Enrico di Robilant ne *Il diritto nella società industriale*, accanto "alla normazione emanante dal potere politico", sia sul piano nazionale sia internazionale, è venuta prendendo forma "la normazione emanante dai centri di potere economico, sociale e d'informazione, grandi o piccoli che siano" (di Robilant 1973: 227). Questo processo, che è venuto intensificandosi nel corso degli ultimi decenni, ha fatto tuttavia sorgere un duplice ordine di problemi che attengono, in qualche caso, alla linea di confine tra il vecchio monopolista delle fonti e il nuovo diritto transnazionale "oltre" gli stati, altre volte, invece, al modo in cui intendere l'idea stessa di un diritto transnazionale "senza" gli stati.

Sul primo fronte, c'è una sottile linea che separa il diritto transnazionale "oltre" gli stati da quello "senza" i medesimi: come si è notato nel paragrafo precedente, mentre alcuni ordinamenti, come quello di eBay, possono entrare in contatto con le giurisdizioni dei sistemi giuridici nazionali, all'atto pratico, nondimeno, tale eventualità costituisce l'eccezione, piuttosto che la regola, nel rapporto tra i due ordinamenti. Ciò non toglie che altre società, come per esempio Amazon, ossia il popolare sito per la vendita di libri, film, musica e altro ancora online, preferiscano ottemperare a molte delle disposizioni dei sistemi giuridici nazionali, come quello inglese (v. Reed 2012: 77); sebbene, a rigore, tali misure non potrebbero esserle imposte sulla base della minaccia di sanzioni. Come già nel caso del diritto soffice (§ 4.3.3.1), i motivi della conformità possono essere i più vari: prestigio, convenienza, immagine o perfino ragioni d'ordine morale. Ma, la sottile linea che distingue il diritto transnazionale "oltre" o "senza" gli stati, sta a ricordare come la minaccia di sanzioni da parte dell'ordinamento non rappresenti l'elemento determinante, o quello principale, grazie al quale dar conto dell'essenza del fenomeno giuridico o di come gli ordinamenti spesso funzionino al giorno d'oggi.

Sul secondo fronte, abbiamo visto casi in cui il funzionamento del diritto transnazionale debba convenientemente intendersi come un diritto "senza" lo stato: ciò è emerso sia con l'esempio d'ICANN e le sue competenze per il dominio dei nomi e con la numerazione per internet (§ 3.4.2.1), sia, in parte, con i profili sostanziali e procedurali della *lex mercatoria* (§ 4.3.3.2), che hanno indotto qualche studioso a denunciare l'odierno diritto commerciale transnazionale come un nuovo imperialismo giuridico che accentua la contrapposizione tra il "nord" e il "sud" del mondo,

tra gli abbienti e i poveri del pianeta. Senza entrare nel merito di quest'ultima discussione (si v. Delazay e Garth 1996), l'esistenza di un diritto senza lo stato solleva tuttavia tre nuovi ordini di problemi, sui quali vale la pena di attirare l'attenzione.

Innanzitutto, come spesso notato dagli studiosi in tema di fonti del diritto, a proposito della parentela tra norme consuetudinarie, fonti fatto e rivoluzioni (Crisafulli 1976: 1032), un diritto senza lo stato può facilmente tramutarsi in un diritto contro lo stato. Come si è insistito più volte nel capitolo presente, la redistribuzione delle fonti all'interno del sistema giuridico s'intreccia con questioni di potere, per le quali, ora, può essere lo stato a tentare di riappropriarsi delle fonti in questione, come nell'esempio d'ICANN, ora, i nuovi centri di produzione normativa possono continuare a erodere il precedente monopolio delle fonti, come sancito dal modello di Westfalia.

Questa doppia possibilità introduce il secondo ordine di questioni, vale a dire come giudicare le tendenze in atto: mentre, nel caso della governance d'internet, si può ben guardare con sospetto al tentativo degli stati, anche per il tramite delle organizzazioni internazionali sotto il loro diretto controllo, di assoggettare per intanto il "livello logico" della rete (§ 3.4.2 (ii)), possono del pari comprendersi alcune delle preoccupazioni di chi ha inteso denunciare volta per volta, i nuovi centri di potere, tramutatisi in fonti, secondo una deriva oligarchica, tecnocratica o, genericamente, anti-democratica, con cui abbiamo esordito nel capitolo precedente.

Di qui, si giunge al terzo e ultimo ordine di problemi, riguardante il complessivo assetto istituzionale. La dinamica dei processi in corso, che ha condotto dalle tradizionali forme di governo a quelle attuali della governance, si è, per così dire, cristallizzata nelle 30 possibili variabili illustrate più sopra con la tavola 6. Come detto, però, a proposito della complessità nella teoria delle reti (§ 2.2.2.1), anche qui vale ciò che Simon definiva come una "struttura gerarchica ben definita", tanto dal punto di vista normativo, quanto da quello fattuale. Passando dal piano delle fonti a quello del disegno istituzionale, bisogna infatti fare i conti sia con le forme in cui le questioni di legittimità, declinate in chiave liberal-democratica con la costituzione dei moderni (§ 3.1.3), sono mutate a contatto con ordinamenti transnazionali oltre o senza lo stato, sia come lo stato sia a sua volta venuto trasformandosi per via della rivoluzione tecnologica. Si tratta del doppio significato secondo cui la formula del "disegno istituzionale" può essere declinata nell'era delle società ICT-dipendenti, secondo un'idea, quella di design, che sarà l'oggetto dell'indagine nel capitolo che segue.

# V.
# *Design*

> "Maggiore la nostra capacità di capire l'esperienza umana, migliore il design che avremo"
>
> Steve JOBS

Abbiamo esaminato, nel corso dei capitoli precedenti, la crescente complessità del fenomeno giuridico (capitolo 2); indotta, o innescata, dalla rivoluzione tecnologica in corso (capitolo 1). Da un lato, si è detto del passaggio dalle tradizionali forme di governo all'odierno reticolo istituzionale, in cui lo stato nazionale appare come uno degli attori, sia pure tra i più rilevanti, dell'arena giuridico-politica della governance (capitolo 3).

D'altro canto, la moltiplicazione di attori, sia pubblici sia privati, sia economici sia sociali, coinvolti nei processi decisionali della governance, è andata di pari passo con la crescente complessità del sistema delle fonti (capitolo 4): dai 3/4 osservabili e 2/3 variabili del sistema di Westfalia (ivi, tavole 2 e 3), siamo giunti ai 6/7 osservabili e 18/30 variabili delle fonti nelle società ICT-dipendenti (tavole 4 e 6).

L'accresciuta complessità delle fonti sottolinea come gli equilibri istituzionali del sistema siano stati ridisegnati a partire dal precedente monopolista delle fonti, ossia lo stato nazionale sovrano. Con la dicotomia moderna d'interno ed esterno, tra "dentro" e "fuori", questo riposizionamento può essere innanzitutto colto sia in chiave centripeta che centrifuga, sia sul fronte del diritto internazionale che di quello interno nazionale; ma, a condizione di aggiungere gli ulteriori processi trasversali del diritto transnazionale. Al posto dell'accentramento tipico del sistema di Westfalia, abbiamo a che fare con un sistema fortemente decentrato; al monismo delle fonti fa da controcanto uno spiccato pluralismo dei fattori produttivi dell'ordinamento. Per comodità, proviamo ora a fissare questa radicale trasformazione, istituzionale e normativa, in ragione di quattro punti principali:

i) il diritto nazionale, sdoppiato nel rapporto tra gubernaculum e iurisdictio, si apre al proprio interno all'insieme delle forze regolatrici che fanno capo ora all'economia (contratti), ora alle norme sociali (consuetudini); che, tuttavia, con la rivoluzione tecnologica, acquistano spesso valenza transnazionale;

ii) il diritto nazionale si apre inoltre a forme di coordinamento e organizzazione internazionali, secondo un processo che si è consolidato progressivamente dalla seconda metà del secolo scorso, favorito dalla crescente complessità dei problemi che

attengono alla totalità del sistema e che porta, tra le altre cose, a un nuovo ruolo della iurisdictio sconosciuto nel precedente modello;

iii) al diritto nazionale si affiancano, come detto, le nuove fonti transnazionali del diritto, la cui autorità, nondimeno, spesso non dipende da un presunto contratto sociale; ma, bensì, dall'accordo della comunità di riferimento che quelle regole siano appropriate a disciplinarne le interazioni;

iv) alla natura del diritto transnazionale "oltre" lo stato, come fonte *extra ordinem* del sistema, vanno aggiunti i casi di un diritto globale "senza" lo stato, o come fonte *contra ordinem* odierna, che si riflette negli scontri tra diritto nazionale e transnazionale, tra quest'ultimo diritto e il diritto internazionale, sui quattro fronti del gubernaculum, della iurisdictio, dei contratti e delle norme sociali.

A ribadire la complessità dei fenomeni in corso, tuttavia, occorre avvertire che il quadro così delineato, non è ancora completo. In fondo, sin dal capitolo primo (§ 1.4.3), abbiamo notato come, alla consueta rappresentazione del diritto come tecnica imperniata sulla minaccia di misure coercitive, secondo la nota formula "se A, allora B", sia venuta subentrando l'idea di immettere le regole del diritto negli ambienti, spazi o oggetti che mediano l'interazione degli individui. Ciò significa che lo spettro della nostra indagine sui diritti nazionale, internazionale e transnazionale, in funzione dei dualismi relativi sia alla taxis (gubernaculum e iurisdictio), sia al kosmos (contratti e consuetudini), deve essere ora approfondito in rapporto ai temi del design, ossia, con l'intento di plasmare la forma di prodotti e processi, così come la struttura di spazi e luoghi, al fine di ottenere una serie di risultati predeterminati, o di prestazioni desiderate.

L'idea, va da sé, non è nuova: è sufficiente pensare all'impiego dei dossi nei fondi stradali per ridurre la velocità delle automobili e far rispettare in questo modo il comando della legge che prescrive, ad esempio, di non oltrepassare i cinquanta chilometri orari in una data zona. Si tratta di un modo alternativo, ma efficace, rispetto a quello tradizionale di far rispettare la legge sulla base della minaccia di sanzioni, specie se, poi, si considera la proverbiale inclinazione dell'automobilista italiano di interpretare le norme del codice della strada, con buona pace di Hobbes, più come una specie di consiglio, che di un vero e proprio comando!

Inoltre, come rimarcato a più riprese nelle pagine precedenti (§§ 2.2.2, 3.1.3.1 (iv) e 4.3.3.1), la scala dei problemi fa ancora una volta la differenza: tanto più, infatti, le società diventano ICT-dipendenti, tanto più gli attori pubblici e privati della governance si affideranno al design per cercare non solo di porre rimedio alla crescente inefficacia del tradizionale intervento coattivo degli stati negli ambienti digitali; ma, per affrontare del pari le sfide del diritto soffice, dei contratti e delle norme sociali in rete, ecc. Per trattare l'insieme di questioni che il design propone, coinvolgendo potenzialmente tutti i settori del diritto fin qui analizzati, il presente capitolo è perciò suddiviso in cinque parti, che integrano in sostanza ciò che si è introdotto fin dal § 1.1.3, a proposito delle modalità del diritto come meta-tecnologia (si v. ivi, figura 3). Osservabili e variabili dell'indagine sono illustrati a continuazione con un nuovo schema:

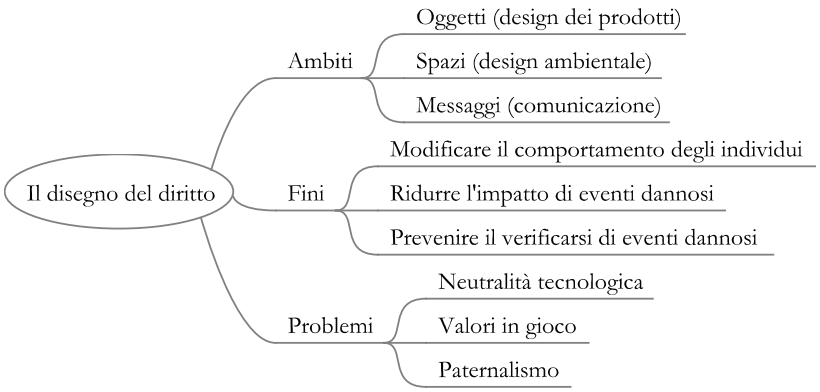


Figura 16: *Campi, finalità e nodi giuridici del design*

Alla luce della figura 16, l'attenzione verterà innanzitutto sugli ambiti del design (§ 5.1): con le indicazioni dello studioso, poeta e designer inglese Norman Potter (1923-1995), il riferimento va rispettivamente agli oggetti, spazi e messaggi intesi come design dei prodotti (§ 5.1.1), dell'ambiente (§ 5.1.2), e della comunicazione (§ 5.1.3).

In secondo luogo, l'accento cadrà sui fini, piuttosto che sugli ambiti del design (§ 5.2): si può mirare a plasmare la forma di prodotti e processi, così come la struttura di spazi e luoghi, ora al fine di modificare il comportamento degli individui (§ 5.2.1), ora con lo scopo di ridurre l'impatto di eventi dannosi (§ 5.2.2); o, di prevenire del tutto la possibilità che quel presunto evento dannoso si verifichi (§ 5.2.3).

In terzo luogo, il capitolo s'incentrerà sui dilemmi e problemi del design (§ 5.3): essi concernono principalmente la neutralità tecnologica delle scelte giuridiche (§ 5.3.1), in rapporto ai valori in gioco (§ 5.3.2), e ai connessi rischi di paternalismo (§ 5.3.3).

Su queste basi – che, poi, sono date dai 3 osservabili e le 9 variabili della figura 16 – il capitolo si soffermerà con particolare attenzione su una particolare figura del design, cioè a dire l'uso delle "tecnologie auto-applicantisi" (§ 5.4). La ragione dipende dal fatto che l'impiego di queste tecnologie, volte alla prevenzione di presunti eventi dannosi, non soltanto solleva gravi questioni di paternalismo, intaccando alcuni assunti chiave dello stato di diritto; ma gode perfino di estremo favore tra alcuni attori, pubblici e privati, dell'odierna governance.

Infine, il capitolo si concluderà, avendo di mira non più una particolare figura del design ma, bensì, uno specifico settore del diritto che illustra concretamente alcune delle sfide del design, ossia il campo della privacy (§ 5.5). In questo modo, saremo introdotti a quella che, idealmente, rappresenta la seconda parte del presente volume, dedicata ai temi della riservatezza informazionale e la tutela dei dati personali.

## 5.1. *Gli ambiti del design*

Abbiamo già avuto modo di ricordare in precedenza (§ 1.4.1), l'opera del premio Nobel statunitense Herbert Simon, il quale, fin dalla prima edizione de *Le scienze dell'artificiale* nel 1969, lamentava lo stato di abbandono, teoretico e accademico, in cui versava la "scienza del design". Con le parole di Simon, "rispetto alle norme prevalenti, la rispettabilità accademica esige che le materie trattate debbano essere intellettualmente robuste, analitiche, formalizzabili ed insegnabili. Nel passato, molto, se non la maggior parte, di ciò che sapevamo attorno al design e le scienze artificiali era intellettualmente sommesso, intuitivo, informale e artigianale" (ed. 1996: 112).

Questo stato di arretratezza, a giudizio di Simon, avrebbe cominciato a essere superato a partire dalla metà degli anni settanta del secolo scorso, con la fondazione del *Design Research Center* presso la Carnegie Mellon University. Oltre alle ragioni istituzionali di un piano carriera del settore, c'era però anche un motivo scientifico alla base dell'irrobustimento della disciplina: il fatto che fosse venuta emergendo e consolidandosi una vera e propria "scienza del design", s'intrecciava ai progressi dell'informatica e allo sviluppo dell'intelligenza artificiale. "In sostanza, la teoria del design mira ad ampliare le capacità dei computer nel dare aiuto al design, attingendo ai mezzi della intelligenza artificiale e della ricerca operativa" (Simon 1996: 114).

Tuttavia, ancora alla fine dello scorso secolo, era il turno di un giurista americano, Lawrence Lessig (n. 1961), per stigmatizzare come, malgrado il ruolo cruciale svolto dall'architettura, o "codice", nel perseguimento di finalità sociali o collettive, i giuristi avessero per lo più riservato la loro attenzione al ruolo svolto dalla legge, dall'economia o dalle norme sociali, nella disciplina dei nuovi ambienti digitali, o cyberspazio. Già fin dal titolo della sua famosa opera, *Codice e altre leggi del cyberspazio* (1999), Lessig mirava invece a rimarcare il ruolo, per molti versi preponderante, dei codici informatici nella regolazione e disciplina dei rapporti individuali. Tra i tanti esempi, si rifletta ancora sull'uso dei DRM (*digital rights management*), cui si è fatto cenno nel capitolo primo (§ 1.4.3): alla tecnica tradizionale del diritto, come insieme di comandi supportato dalla minaccia di misure coercitive, si affianca – e, per molti versi, subentra – il disegno di ambienti e architetture digitali, fondati su codici informatici, che determinerebbero a priori quello che si può, o non si può fare, nel cyberspazio.

Nel giro di pochi anni a partire dal volume di Lessig, questa linea di ricerca si è estesa a numerosi campi dell'ordinamento giuridico, comprendendo la tutela dei dati personali e il consenso informato, l'usabilità universale dei mezzi informatici e la giustizia sociale, il controllo del crimine e gli strumenti fondati sul design per la implementazione delle politiche sociali, e così via. Sebbene, con la consueta prudenza dei giuristi, il tema abbia tardato ad attrarre l'attenzione degli esperti nel campo del diritto, lo studio dei profili regolativi della tecnologia è diventato progressivamente popolare. Quanto più il processo di ICT-dipendenza delle società odierne si consolida, tanto maggiore è il ruolo che il design è chiamato a svolgere, ora, affianco alle consuete forme regolative del diritto, dell'economia o delle norme sociali, ora, in sostituzione delle stesse. Questa popolarità del tema, com'è altrettanto comprensibile, ha tuttavia il proprio prezzo, e cioè la difficoltà di orientarsi nella pletora di ri-

cerche incentrate sull'impatto che il design, l'architettura o i codici, hanno nel mondo del diritto.

Come riferito poc'anzi, nell'introduzione del presente capitolo, un primo modo per orientarsi però esiste, e consiste nel seguire le indicazioni di un noto designer come Norman Potter. In *Cos'è un designer*, la cui prima edizione appare significativamente lo stesso anno de *Le scienze dell'artificiale* di Simon (1969), Potter consigliava di distinguere tra "design di prodotto (oggetti), design ambientale (luoghi) e design di comunicazione (messaggi). Sono categorie entro le quali sfumano ulteriori e necessarie distinzioni (come per esempio la differenza tra il design di attrezzature industriali e quello di prodotti di dettaglio destinati al mercato locale) ma rappresentano comunque un valido punto di partenza" (Potter ed. 2010: 4).

Seguendo i consigli dello studioso inglese, inoltriamoci nello studio giuridico del design.

### 5.1.1. *Prodotti*

La prima classe di variabili della nostra indagine sul design giuridico è forse quella con la quale i lettori hanno maggiore dimestichezza: il design dei prodotti come il vostro smartphone o tablet, il design delle automobili, dei frigoriferi e via dicendo. Esiste in materia una letteratura sterminata; ma, per i lettori interessati, mi limito a segnalare un volume dello psicologo e scienziato americano Donald Norman (n. 1935), *Il design delle cose quotidiane*, apparso nel 1988, dalla copertina geniale: una caffettiera disegnata in modo tale che, comunque vogliate versare il caffè, non potrete che rovesciarvelo addosso! [1].

Oltre al disegno degli oggetti della vita quotidiana, abbiamo anche il disegno di processi, più che di prodotti: ad esempio, il disegno di una linea di montaggio industriale robotizzata. A partire dai primi esperimenti nel settore manifatturiero e automobilistico, come nel caso dell'UNIMATE robot introdotto dalla General Motors nei suoi impianti del New Jersey nel 1961, si pensi a come, neanche vent'anni dopo, l'industria automobilistica giapponese abbia rivoluzionato il settore, ridisegnando le linee di produzione, abbattendo i costi e migliorando la qualità delle proprie macchine, tramite l'introduzione di robot su larga scala (Pagallo 2013: viii).

Ma, che dire del design giuridico dei prodotti e dei processi produttivi?

Anche qui, per cominciare a cogliere la complessità del tema, basti un esempio: si tratta dei sistemi informativi negli ospedali che devono trattare i dati dei pazienti in modo tale che, tra le altre cose, il loro nome sia separato dai dati relativi ai trattamenti medici o al loro stato di salute. Fin dal documento del 2009 sul "futuro della privacy" (doc. WP 168), le Autorità garanti europee hanno raccomandato, in ossequio ai principi della controllabilità e confidenzialità relativa al trattamento dei dati, che gli identificatori biometrici "devono essere messi sotto il controllo degli interessati (tramite tessere elettroniche, ad esempio), piuttosto che custodite in banche dati esterne" (*op. cit.*, § 52, p. 14).

---

[1] La traduzione italiana del volume, non a caso, suona *La caffettiera del masochista. Psicopatologia degli oggetti quotidiani*, più volte ristampato a partire dal 1990 (nuova ed. 2009).

Tuttavia, il design degli oggetti non riguarda soltanto processi e prodotti artificiali perché, a ben pensarci, esso coinvolge anche gli organismi biologici. È il caso di piante o animali geneticamente modificati (OGM), come avviene con i salmoni norvegesi che, penso, qualche lettore avrà certamente addentato. Ai fini giuridici, il riferimento va, in questo contesto, a tutte le disposizioni normative che disciplinano il settore, come nel caso della direttiva 18 del 2001 in Europa.

Infine, un richiamo va all'odierno dibattito sul post-umano e i cyborg, vale a dire la possibilità stessa di ridisegnare l'organismo umano. Si tratta di un tema estremamente popolare nei film di fantascienza, come nell'esempio di *Minority Report* (2002), in cui il protagonista, Tom Cruise, è costretto a comprare al mercato nero un paio di bulbi oculari per sfuggire alla cattura del nemico. Sebbene, come noto agli esperti di bioetica, alcuni di questi scenari vadano tramutandosi in realtà, possiamo nondimeno tralasciare l'argomento in questa sede.

### 5.1.2. *Ambienti*

La seconda serie di variabili della nostra indagine riguarda il disegno degli ambienti, ossia dei luoghi e degli spazi in cui viviamo e interagiamo. Nell'era predigitale, un esempio di scuola era dato dai ponti di Long Island, costruiti in modo tale da bloccare il transito degli autobus verso New York City. Al giorno d'oggi, conviene piuttosto fare attenzione alla progettazione di luoghi quali gli aeroporti, i centri commerciali o la rete autostradale, che, tempo addietro, un etnologo e antropologo francese, Marc Augé (n. 1935), ha sintetizzato con l'espressione di "non luoghi". In contrapposizione agli spazi identitari, relazionali e storici, il disegno di questi nuovi ambienti corrisponderebbe ai fenomeni contemporanei della massificazione, dell'anonimato e della solitudine; ambiti a cui, peraltro, si accede paradossalmente, solo fornendo la prova della propria identità con il passaporto o la carta di credito (Augé ed. 2009).

Senza entrare nel merito di quest'ultima analisi, tuttavia, andrebbe aggiunto come la tecnologia sia andata trasformando gli stessi tradizionali luoghi storici della relazionalità e degli spazi identitari. Basti far caso all'uso dilagante delle telecamere di sorveglianza a circuito chiuso (CCTV), per cui, dalle strade alle piazze, dagli stadi all'università, dai musei alle banche, la ripresa automatizzata di sempre più vasti spazi, pubblici e privati, sta mutando, in modo anche drammatico, la natura stessa delle città. Si tratta di una evoluzione del design ambientale che va di pari passo con esigenze di natura giuridica, dato che lo scopo del monitoraggio permanente delle persone e delle cose si giustifica con il fine di garantire la sicurezza negli aeroporti, nelle metropolitane, nelle stazioni, nei parcheggi, ecc. Sebbene rimanga il problema di appurare empiricamente l'effettività dei dispositivi CCTV nel prevenire o reprimere il crimine, non è detto, poi, che non esistano accorgimenti per tutelare i diritti delle persone: nel documento sul futuro della privacy, richiamato nel paragrafo precedente, le Autorità garanti europee, ad esempio, hanno suggerito di progettare i sistemi di videosorveglianza nella rete dei trasporti pubblici, in maniera tale che le facce degli individui non siano riconoscibili. Siccome, però, avremo modo di tornare sulla questione nella seconda parte del presente volume in tema di tutela dei dati personali e della privacy informazionale, sia sufficiente, per ora, questi brevi cenni al tema dell'impatto del design ambientale.

### 5.1.3. *Messaggi*

L'ultimo insieme di variabili sugli ambiti del design, dopo i prodotti e gli ambienti, concerne il design dei messaggi o della comunicazione. Il settore in cui tale forma di design la fa da padrona, è certamente quello della pubblicità e della propaganda politica; anche se, bisognerebbe aggiungere, il principio si applica pure ad alcuni convegni internazionali, in cui lo spazio per molte relazioni è spesso ridotto al lasso di un quarto d'ora. Qui, se mai ci fosse qualche buona idea in una relazione, la si dovrebbe pur sempre poter stampare come messaggio succinto su una t-shirt!

Anche nell'ambito della comunicazione, il ruolo della tecnologia è determinante: prova ne sia le peripezie di una nota piattaforma sociale quale Facebook, a proposito dei termini di servizio e controlli sulla privacy. Tra i tanti casi possibili, basti segnalare come, nel febbraio 2009, Facebook avesse annunciato la propria intenzione di modificare i termini di servizio, rivendicando la proprietà sui materiali, quali foto e video, postati sul sito, salvo poi fare marcia indietro pochi giorni dopo, a causa della protesta degli utenti. Significativamente, un anno dopo, nel maggio 2010, Facebook comunicava di aver "drasticamente semplificato e migliorato i propri controlli sulla privacy" che, prima, prevedevano ben 170 opzioni differenti con 50 possibili configurazioni del sistema. Il flusso dei messaggi veniva pertanto ridisegnato in modo tale da registrare soltanto il nome, profilo, genere e reti sociali dell'utente, mentre gli "amici" non sarebbero stati più inclusi automaticamente nel flusso di informazioni e, a loro volta, le applicazioni della piattaforma, come i giochi, avrebbero potuto finalmente essere disattivate. Nel novembre 2012, tuttavia, Facebook cambiava nuovamente avviso, mettendo mano sia alla propria normativa sull'utilizzo dei dati, sia alla dichiarazione dei diritti e delle responsabilità con cui, in pratica, si privava gli utenti del diritto di voto che era stato fin lì riconosciuto per determinate materie della piattaforma sociale.

Senza dover ulteriormente esaminare il regime giuridico del sito, il caso di Facebook è però particolarmente istruttivo per cogliere la specifica complessità del design relativo ai messaggi, o comunicazione.

In primo luogo, dal piano informativo cui si è fatto cenno nel capitolo secondo (§ 2.1), siamo passati al piano comunicativo dei messaggi tra un emittente e un ricevente che, a sua volta, reagisce a tali messaggi secondo l'effetto di retroazione o *feedback* (su cui ancora § 2.3.1, in tema di cibernetica giuridica).

In secondo luogo, l'accento va posto sul disegno del mezzo attraverso il quale si attua la comunicazione. Lungi dall'essere un semplice strumento, il medium, secondo la celebre definizione del sociologo canadese Marshall McLuhan (1911-1980), è esso stesso il messaggio, nel senso che piega a sé, o ricurva, il contenuto di ciò che il mittente intende comunicare. Al lettore scettico, basti ricordare la distanza che passa tra mandare un sms, un whats-app o una mail, tra una telefonata tradizionale e una via Skype.

In terzo luogo, è il caso di adottare un approccio olistico e, cioè, di inquadrare l'insieme degli emittenti e dei riceventi, secondo il feedback, il medium e i contenuti dei messaggi tramite un design istituzionale. Ancor più della dichiarazione dei diritti e delle responsabilità in Facebook, il richiamo va all'opera dei padri fondatori statunitensi (§ 3.1.3.1); così come alle difficoltà d'intendere quale sia mai il disegno istituzionale dell'Unione europea (§ 4.3.2.1). Si tratta dei temi che abbiamo anche

affrontato dal punto di vista degli equilibri interni all'odierna governance, tra rappresentanza politica e decisioni giuridiche (§ 3.4.3); che, in quel contesto, abbiamo svolto in chiave procedurale.

In questa sede, per approfondire ulteriormente la questione e capire in che modo la rivoluzione tecnologica stia incidendo, per il tramite del design, sugli ordinamenti contemporanei, occorre dedicare speciale attenzione al secondo osservabile della nostra analisi; e chiedersi, dopo gli ambiti del design, quale possa esserne lo scopo.

## 5.2. *I fini del design*

Ci sono molteplici modi in cui il design può incidere sul comportamento delle persone: 101 per l'esattezza, secondo un articolo di Lockton, Harrison e Stanton (2010), sul design dei prodotti.

Qui, però, è sufficiente prendere spunto dalla distinzione che Norberto Bobbio faceva tra la funzione "promozionale" e quella "repressiva" del diritto, per cui la nota formula di Kelsen, "se A, allora B" (v. § 1.1.3), non deve essere necessariamente declinata in chiave di sanzioni, o misure, coercitive ("B"), ma altresì di sanzioni positive come gli incentivi (Bobbio 1977).

Su queste basi, possiamo delineare tre diverse finalità per le quali si può pensare di plasmare la forma delle norme e delle istituzioni, vale a dire dei prodotti e dei processi, così come la struttura degli spazi e dei luoghi, per il tramite del design:

i) in omaggio alla funzione promozionale del diritto, il design può spingere gli individui a cambiare il proprio comportamento;

ii) in rapporto alla tradizionale funzione repressiva del diritto, il design può mirare a prevenire la possibilità che un presunto evento dannoso si verifichi;

iii) tra i due estremi, il design può infine avere l'obiettivo di ridurre l'impatto degli eventi dannosi.

Per illustrare sin d'ora questi diversi scopi del design, torna utile l'esempio dei dossi stradali, richiamato nell'introduzione del presente capitolo. Il design dei dossi può infatti essere ricondotto alla prima modalità del design, come forma per invogliare un comportamento più prudente da parte delle persone: perfino il più incallito automobilista italiano emulo di Hamilton o Alonso, ci penserà su due volte prima di sfrecciare a centoventi in una strada nella quale egli sa che corre il rischio di sfasciare la propria macchina!

Quanto alla seconda modalità del design e rimanendo nell'universo delle auto, l'obiettivo di garantire una prevenzione totale degli eventi dannosi è materializzato dalle prime macchine intelligenti in grado di arrestarsi, o di ridurre la velocità, a seconda che siate stanchi o ubriachi oppure delle congiunture dell'ambiente circostante. Nonostante le proteste di coloro i quali amano guidare in piena autonomia la propria macchina, la funzione preventiva dei veicoli robotici non sembra del tutto una cattiva idea, se solo si pensa che, ogni anno in Europa, ci sono circa 1.300.000 incidenti e 41 mila morti sulle strade.

Infine, a metà strada tra i primi due obiettivi del design, troviamo gli *air-bag* come mezzo per ridurre l'impatto degli incidenti stradali.

La rivoluzione tecnologica ha naturalmente ampliato lo spettro delle applicazioni in cui i disposti della legge e i fini delle istituzioni sono immessi nei prodotti, ambienti e messaggi del design, al fine di ottenere determinati risultati o una serie di prestazioni desiderate. Proseguiamo pertanto la nostra indagine, esaminando più in profondità il primo scopo "promozionale" del design.

### 5.2.1. *Sanzioni positive*

L'intento promozionale del design, volto a incoraggiare gli individui a modificare il proprio comportamento, può essere chiarito attraverso una nutrita schiera di esempi. Per cominciare, torniamo ai sistemi per la condivisione dei file sulla rete di internet, noti come peer-to-peer (P2P), introdotti sin dal capitolo primo (§ 1.2). Uno dei maggiori problemi che affligge queste reti di condivisione, ignorando per il momento la questione della violazione del diritto d'autore, concerne il fenomeno degli scrocconi – ciò che in inglese viene reso con l'espressione "free riding" – per cui buona parte degli utenti delle reti P2P tende a usare questi sistemi per procacciarsi informazione e scaricare i file preferiti, siano essi musica, o video, o altro ancora, senza però contribuire in alcun modo al funzionamento del sistema: ad esempio, caricando a loro volta file musicali o video.

Questo comportamento egoistico è peraltro favorito da alcune caratteristiche di questi sistemi, quali l'anonimia degli utenti e la difficile tracciabilità dei nodi. Davanti alla possibilità concreta che il sistema collassi per l'egoismo degli utenti, i disegnatori delle applicazioni P2P hanno dovuto per ciò correre ai ripari, facendo leva, ora, su incentivi basati sulla fiducia, come nel caso dei meccanismi di reputazione e punteggi che abbiamo già visto all'opera con eBay (§ 4.3.3.2); ora, offrendo servizi in cambio di una maggiore collaborazione; oppure, diminuendo semplicemente la connettività dell'utente che non aiuti al processo di condivisione dei file. Due popolari applicazioni P2P, come µTorrent e Azureus/Vuze, hanno implementato dei meccanismi anti-sanguisughe che rallentano la velocità di scaricamento degli utenti, se il loro grado di condivisione risulta troppo basso.

Affianco a queste forme di baratto digitale, un ruolo crescente viene poi svolto, come detto, dal giudizio dei pari e di altri utenti in rete, per via delle proprie recensioni a proposito di ristoranti, alberghi, viaggi turistici, noleggio macchine e altro ancora. Mentre, nel caso già menzionato di eBay, la società californiana premia i venditori di maggior successo, nel rispetto delle regole e condizioni di servizio del sito, assegnando loro il grado di *Power Seller*, secondo cinque livelli che vanno dal bronzo al titanio, simili regole sono seguite anche da altri siti, come *Trip Advisor*, che a sua volta premia gli utenti con una serie di distintivi, a seconda del numero di riscontri positivi che hanno fatto séguito alle proprie recensioni. Si tratta in fondo di una serie di accorgimenti per cui, tramite il design dei propri servizi, i siti incoraggiano l'adozione di un codice di comportamento da parte degli individui, compendiato con il neologismo della "netiquette", che dovrebbe rappresentare il termine di riferimento per l'uso delle varie forme di comunicazione e di interazione in rete.

Inoltre, un modo ulteriore in cui il design può indurre gli individui a modificare il proprio comportamento riguarda la forma in cui si dà lo spettro delle scelte pos-

sibili: un esempio di scuola riguarda l'esposizione dei prodotti in un supermercato o nel caffè universitario, mettendo in bella vista i prodotti alimentari più sani e il cibo spazzatura negli angoli più riposti del locale, così da invogliare gli individui a consumare i primi, più che il secondo tipo di prodotti (Thaler e Sunstein 2009).

Lo stesso principio si applica al disegno delle pagine web e degli interfaccia informatici, dove l'intento è d'invogliare un dato comportamento nell'utente, pur rispettandone la libertà di scelta. Tra i meccanismi a disposizione, è il caso della configurazione di base del sistema, impostata in forma tale da dare priorità a determinati possibili usi del sistema stesso. È una modalità del design che va di pari passo con il disegno d'interfaccia informatici che dovrebbero essere "intuitivi" per l'utente o, come suole dirsi, *user friendly*; e che s'intreccia con l'ulteriore finalità del design che ha di mira la sicurezza degli individui. A poco varrebbe, in fondo, il tentativo di modificarne il comportamento se il design non fosse poi in grado di far comprendere agli interessati il senso delle proprie operazioni. Lasciando per ora da parte questo intreccio tra trasparenza ed efficienza del design, bisogna passare a questo punto all'esame della seconda variabile relativa ai suoi fini. Dopo quello promozionale delle sanzioni positive tramite incentivi, scambi, baratti digitali, ecc., occorre esaminare il fine normativo e istituzionale della sicurezza.

### 5.2.2. *Misure di sicurezza*

Il tema della sicurezza tramite design deve essere innanzitutto distinto secondo due accezioni: da un lato, l'intento è quello di prevenire il verificarsi di eventi dannosi; dall'altro, lo scopo è quello di attenuare l'impatto di questi eventi, una volta che gli stessi si verifichino. Per comodità espositiva, partiremo da quest'ultimo punto, a metà tra le funzioni promozionali e repressive del diritto evidenziate da Bobbio (§ 5.2); per poi passare, nel prossimo paragrafo (§ 5.2.3), allo studio del design come tecnologia auto-attuantesi, o del controllo totale.

Anche a delimitare in questo modo il senso della sicurezza tramite il design, bisogna tuttavia distinguere due ulteriori accezioni del termine che la lingua inglese, a differenza dell'italiano, consente di chiarire. Per un verso, possiamo declinare la sicurezza come *safety*, vale a dire come condizione il cui venir meno può recarci un danno diretto o immediato. Da questo primo punto di vista, lo scopo del design di attenuare l'impatto di possibili eventi dannosi s'intreccia con ciò che è stato detto nel paragrafo precedente, sul disegno d'interfaccia informatici che dovrebbero essere *user friendly*. La configurazione di base degli interfaccia e dei sistemi informatici dovrebbe infatti garantire che i valori del design siano appropriati anche per i novellini e, però, che il sistema sia comunque in grado di aumentare la propria efficienza (Kesan e Shah 2006). È il caso dell'inserimento di collegamenti semplici ed efficaci per la richiesta d'informazioni o l'inoltro di reclami da parte degli interessati, impostando al contempo il sistema in modo tale che, modificando l'interfaccia con l'aumento o la diminuzione della preminenza data a una configurazione di base, l'utente sia in grado di usare il programma informatico nel modo che ritiene più appropriato. Per esempio, prima ancora di premere inopinatamente un tasto del sistema – azione che ci rovinerebbe, cancellando, per esempio, informazioni preziose – il sistema dovrebbe essere in grado di avvertirci di quello che stiamo per fare!

D'altra parte, possiamo intendere la sicurezza nel senso della *security*, più che della *safety*, ossia come condizione il cui venir meno può mettere in condizione altri, oppure, rendere loro più facile, di recarci danno. Si pensi, ancora una volta, ai sistemi informativi degli ospedali, in cui il nome dei pazienti è tenuto separato dai dati relativi ai trattamenti medici o al loro stato di salute (§ 5.1.1). Il fine di questo tipo di design è certamente quello della sicurezza; ma, non nel senso di dover prevenire che qualcuno possa introdursi nel sistema informativo, bensì, che quel qualcuno, anche essendosi introdotto illecitamente nel sistema, non possa incrociare i dati relativi ai nomi dei pazienti con quelli del loro stato di salute. Analogo discorso vale per altri accorgimenti in tema di sicurezza come le copie di riserva o "backup". L'obiettivo di questa modalità del design non è, ancora una volta, d'impedire che un dato evento dannoso si verifichi: piuttosto, il problema che ci si pone è che qualora malauguratamente questo evento si materializzi, il sistema sia preparato a tutelarsi, né più né meno come occorre allorché gli airbag delle macchine sono tenuti a funzionare per salvare delle vite umane nei casi d'incidenti. Così, tornando all'ipotesi delle misure di sicurezza relative alle copie di scorta o di riserva, il problema non consiste nell'evitare che l'informazione vada distrutta ma, bensì, nel caso in cui tale evento sventuratamente si verifichi, di essere preparati per correre ai ripari.

La distinzione tra questi due piani di sicurezza è cruciale perché, negli esempi dati in questo paragrafo, la tecnica del design non incide direttamente sul comportamento degli individui, a differenza di quanto visto nel precedente paragrafo e di ciò che diremo in quello successivo. Qui, le responsabilità del designer riguardano infatti l'affidabilità e meticolosità tecnica del progetto, più che le sue ricadute sulla autonomia degli individui. Si tratta di una differenza critica, su cui avremo modo di insistere più sotto, a proposito dei problemi del design in tema di paternalismo (si v. § 5.3.3).

Ma, proprio per via di questa distinzione, occorre ora passare in rassegna il terzo e ultimo fine del design; quello, cioè, che mira a prevenire la possibilità che gli eventi dannosi si verifichino.

### 5.2.3. *Controllo totale*

Abbiamo riferito fin dal capitolo primo (§ 1.4.3), uno degli aspetti più rilevanti della rivoluzione tecnologica dal punto di vista giuridico, ossia come il canonico modo di concepire il diritto come insieme di regole supportate dalla minaccia di sanzioni fisiche, risulti più spesso inefficace nel mondo di internet. Nel capitolo quarto (§ 4.3.3.1), si è poi detto delle ulteriori difficoltà cui questo approccio va incontro in termini di conflitti di competenza e giurisdizione, ammesso, ma non concesso, che i suddetti problemi di efficacia siano stati nel frattempo risolti. Non sorprenderà pertanto che, fin dagli anni novanta del secolo scorso, tanto gli stati quanto le società e imprese private abbiano pensato, nel bene o nel male, di correre ai ripari: tra i primi modi con cui si è provveduto a sopperire alla crescente inefficacia del tradizionale apparato repressivo dello stato, si è già fatto menzione del DRM (§§ 1.4.3 e 5.1). Il riferimento va all'insieme delle tecniche con le quali, nei settori della produzione e vendita di contenuti e supporti digitali, le imprese private hanno mirato all'autotutela dei propri diritti, controllando le modalità di accesso, uso, copia, consultazione, modifica, riproduzione, stampa, ecc., dei loro prodotti.

A loro volta, gli stati non sono certo rimasti a guardare: emblematico l'esempio della Cina, cui si è già fatto cenno (v. § 3.4.2), che ha isolato la propria rete dal resto del pianeta tramite la "grande muraglia di fuoco", sottoponendo altresì i fornitori di servizi internet ad uno stretto controllo statale. Del resto, l'idea di porre rimedio all'inefficacia dell'apparato repressivo dello stato con l'introduzione di un massiccio sistema di filtri in rete, non è appannaggio esclusivo della Cina. Sia pure in forma più moderata, l'idea è stata anche coltivata per un certo tempo dalla Commissione europea: nel suo rapporto del 2010 sullo stato di applicazione della direttiva 48 del 2004, vale a dire la normativa europea sul copyright, leggiamo che "nonostante un miglioramento d'insieme relativo alle procedure di applicazione, il volume complessivo e il valore finanziario delle violazioni dei diritti di proprietà intellettuale sono allarmanti. Una ragione è l'aumento senza precedenti relativo alle opportunità di violare tali diritti che è offerto da internet" [2]. Di qui, per porre fine a questi illeciti, la Commissione raccomandava che i fornitori di servizi in rete (ISP) dovessero essere obbligati dalla legge a istallare "un sistema di filtraggio per tutte le comunicazioni elettroniche" e, specialmente, per le applicazioni P2P. Infine, la Commissione appoggiava una nuova generazione d'ingiunzioni nei confronti degli ISP, indipendentemente dalla loro responsabilità giuridica, al fine di prevenire "ulteriori violazioni" del copyright anche con effetti extra-territoriali.

Per una serie di ragioni politiche e giuridiche, sulle quali avremo occasione di far ritorno nel corso di questo capitolo, la proposta della Commissione, a quei tempi sotto la pressione del presidente di turno dell'Unione, ossia Nicolas Sarkozy (n. 1955), cadde nel vuoto; sebbene, bisogna pur aggiungere che alcuni stati membri, come il Regno Unito, abbiano continuato ad accarezzare l'idea di risolvere, se non tutti, alcuni dei problemi d'internet tramite l'introduzione di un sistema onnipervasivo di filtri. È sufficiente per ora ricordare alcune controverse disposizioni del *Digital Economy Act* (DEA) del 2010 e come, tra il 2013 e il 2014, sotto il governo conservatore di David Cameron (n. 1966), il Regno Unito abbia adottato un ulteriore sistema di filtraggio per il (presunto) controllo della pornografia in rete.

Ma, senza inoltrarci da subito nei dettagli di queste misure, balzano agli occhi due dati fondamentali. Il primo riguarda la differenza con le misure di sicurezza esaminate nel paragrafo precedente: mentre queste ultime avevano l'obiettivo di attenuare l'impatto di eventi dannosi, qui, al contrario, lo scopo del design è quello di prevenire che questi casi dannosi si verifichino. Fatalmente, come capita sovente con le cose umane, i desideri non sempre si avverano: il 23 gennaio 2014, ad esempio, per ben otto ore gli utenti cinesi non sono stati in grado di caricare le pagine web del sistema, inclusi giganti come Baidu, il Google cinese, o Sina.com, dato che la grande muraglia di fuoco aveva fatto fiasco, smistando per errore il traffico cinese d'internet a siti censurati in quel paese, alcuni dei quali connessi a una compagnia con sede in Wyoming, Stati Uniti! [3]

Il secondo elemento di riflessione riguarda invece il senso di questa prevenzione:

---

[2] Si v. SEC-2010-1589, parte finale del documento della Commissione.

[3] Si v. l'articolo del 24 gennaio 2014, *Experts suspect Great Firewall in crash of web in China*, sull'"International New York Times" a p. 13.

più che delineare il livello del rischio riguardo l'accesso indebito ai sistemi o contenuti informativi, o alla manomissione degli stessi, sulla base della probabilità di eventi legati all'interazione umana, l'ambizione, più spesso, è stata di prevenire totalmente questi eventi dannosi in ragione di una presunta infallibile tecnologia automatizzata. Per esprimere la posta in gioco secondo l'ammonimento di Lessig, "i controlli sull'accesso ai contenuti non saranno controlli ratificati dalle corti; i controlli sull'accesso ai contenuti saranno controlli codificati dai programmatori. E laddove i controlli che sono immessi nel nome della legge devono sempre essere sottoposti al controllo di un giudice, i controlli immessi nella tecnologia non hanno in se stessi un simile controllo" (Lessig 2004: 152).

Sulla base di questo avvertimento, possiamo passare ora all'esame dei problemi giuridici del design. Dalle questioni normative legate al design delle leggi, come vedremo, saremo tenuti a fare i conti con i nodi istituzionali del design.

## 5.3. *I dilemmi del design*

Il terzo e ultimo osservabile della figura 16, con cui abbiamo cominciato l'analisi nel presente capitolo, richiede di ricapitolare in tre parti, le tappe dell'indagine che ci ha condotti fino a questo punto.

Nel capitolo primo (figura 3 in § 1.1.3), si è introdotto l'approccio di questo libro nel senso del diritto come meta-tecnologia, precisandone gli osservabili sia a proposito dei livelli, che delle modalità coattive e autoritative dell'intervento giuridico.

Nel capitolo anteriore (tavola 4 di § 4.3), questi osservabili sono stati specificati, da un lato, sul piano del livello d'intervento, con il triplice rimando al diritto nazionale, internazionale e transnazionale. D'altro canto, sul piano delle modalità, l'analisi poco dopo si è soffermata sul rapporto tra le tradizionali forme d'intervento coattivo del legislatore e il cosiddetto diritto soffice (si v. §§ 4.3.1 e 4.3.1.1).

Infine, poc'anzi in questo capitolo (da § 5.2 a 5.2.3), abbiamo aggiornato queste forme d'intervento con la triplice modalità, o fini, che il design può avere ai livelli del diritto precedentemente segnalati. La necessità dell'aggiornamento dipende da quanto detto sin dal capitolo primo, riguardo l'impatto della quarta rivoluzione sulle tecniche del diritto, vale a dire il terzo osservabile della figura 4 in § 1.4. Il ricorso giuridico al design, in altri termini, può essere inteso come la risposta alla crescente inefficacia, alla quale il tradizionale apparato sanzionatorio dello stato è andato incontro per via della rivoluzione tecnologica, per cui si è trattato di rispondere alle sfide della tecnologia con le armi della tecnologia stessa, e cioè immettendo i comandi del diritto nei prodotti e nei processi tecnologici, nei luoghi e negli spazi dell'interazione umana, al fine di far valere i dispositivi della legge.

Sul fronte delle modalità coercitive dell'intervento, abbiamo così visto all'opera, nel paragrafo precedente, il fine del design di prevenire il verificarsi di presunti eventi dannosi, ora sul piano nazionale (i filtri della DEA britannica); ora internazionale (i filtri della Commissione europea); ora transnazionale (i DRM delle imprese del settore). Che l'intervento giuridico sia avvenuto ora da parte delle autorità pubbliche, ora a cura delle compagnie private, non sorprende, avendo a mente il

passaggio dalle tradizionali forme di governo a quelle odierne della governance che comprende, nel bene e nel male, sia attori privati sia organismi pubblici (§ 3.4.2).

Sul fronte, invece, delle modalità d'intervento soffice, il riferimento va alle forme del design che mirano a incoraggiare gli individui a mutare il proprio comportamento con le tecniche degli incentivi, i baratti digitali e, in genere, le forme delle sanzioni positive. Qui, sebbene non manchino esempi nel settore pubblico, è interessante notare come i casi riguardino soprattutto l'ambito transnazionale: P2P, eBay, Trip Advisor, ecc. La ragione è stata sottolineata sin dal capitolo precedente (§ 4.3.3.2), per cui coloro che sono sottomessi all'autorità delle regole che governano la comunità transnazionale, lo fanno attraverso la loro scelta: con la formula inglese, "opt in", insomma, e non "opt out" (come avviene talvolta con gli stati).

Possiamo fissare le premesse dell'indagine del presente paragrafo con una nuova figura:

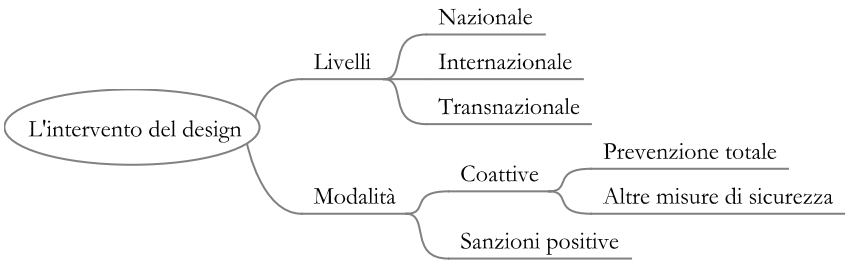


Figura 17: *Il diritto come meta-tecnologia oggi*

Sono tre, come detto, i nodi principali che il nuovo quadro pone e concernono la neutralità tecnologica del diritto, il suo rapporto con i valori in gioco, nonché i rischi del paternalismo. Si tratta di un plesso di questioni che dai nodi normativi del design giuridico conducono agli odierni dilemmi istituzionali del design.

Proseguiamo l'indagine con il primo di questi tre nodi.

### 5.3.1. *La neutralità tecnologica delle scelte giuridiche*

Uno dei problemi cui va incontro il diritto come meta-tecnologia riguarda il fatto che l'intervento del legislatore non dovrebbe né soffocare lo sviluppo tecnologico né richiedere di essere frequentemente rivisto in ragione dello stesso sviluppo della tecnologia. A questi primi due significati della formula relativa alla neutralità tecnologica delle scelte giuridiche se ne affiancano altri: il principio di non discriminazione tra tecnologie con effetti equivalenti, il principio dell'equivalenza funzionale tra attività in rete e mondo offline, fino all'idea di fare attenzione agli effetti e intenzioni del comportamento individuale, più che ai comportamenti astrattamente considerati, o ai mezzi utilizzati, secondo una prospettiva che riconduce a sua volta a un approccio neutrale alle scelte giuridiche in chiave tecnologica (Koops 2006: 83-90).

Altri autori riassumono i principi della neutralità tecnologica secondo tre aspetti: quello dell'indifferenza tecnologica della legge, quello della sua neutralità riguardo

alle forme dell'implementazione e, infine, quello della potenziale neutralità (Reed 2012: 195-199). In particolare, riguardo al profilo dell'indifferenza tecnologica della legge, l'idea è che le finalità perseguite valgano a prescindere dalla tecnologia interessata: nel caso della normativa europea in materia di tutela dei dati personali (si v. § 3.4.1), si pensi alla nozione di trattamento di cui all'articolo 2, lettera b, della D-95/46/CE[4]. Per quanto la definizione, che il lettore trova sotto in nota, sia invecchiata tutto sommato bene, non è un caso che essa, nella proposta di nuovo regolamento per la protezione dei dati, presentata dalla Commissione europea il 25 gennaio 2012, è stata significativamente integrata. La previa formula "con o senza l'ausilio di processi automatizzati e applicate a dati personali" suona ora "applicate a dati personali o insiemi di dati personali" (articolo 4(3) della proposta di regolamento in tema di definizioni). La ragione dipende dal fatto che la normativa ha dovuto fare i conti con una nuova tecnologia che, nel 1995, non esisteva: il "data mining". Si tratta delle tecniche che sono in grado di estrarre e incrociare informazioni da una mole gigantesca di dati, per cui singole tracce digitali che ciascuno di noi lascia dietro di sé, all'apparenza insignificanti, possono diventare a tutti gli effetti dati personali grazie a queste tecniche. Il legislatore europeo ne ha dovuto prendere atto.

In secondo luogo, riguardo alla neutralità relativa alle forme d'implementazione, sono i casi in cui il legislatore fa riferimento a una specifica tecnologia ma, poi, è indifferente alle forme in cui quest'ultima di fatto si materializza. Basti pensare alle firme elettroniche e come queste ultime siano state disciplinate dal legislatore europeo con il combinato disposto degli articoli 2(1)-(2) e 5 della D-1999/93/CE[5]; e come, due anni dopo, nel 2001, la Commissione delle Nazioni Unite sul diritto internazionale commerciale (UNCITRAL), si sia spinta oltre in questa direzione, proponendo una definizione di firma elettronica che, a rigore, può anche valere per le firme tradizionali. Ai sensi dell'articolo 2(a) della legge modello della Commissione, per firma elettronica s'intendono i "dati in forma elettronica che, fissati o associati logicamente a un messaggio di dati, possono essere impiegati per identificare il firmatario con riguardo a un messaggio, o per indicarne l'approvazione dell'informazione contenuta in un messaggio di dati". Da questo punto di vista, la neutralità delle forme d'implementazione di una tecnologia specifica, come quella della firma

[4] Si tratta di "qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione" di informazioni riguardanti la persona interessata.

[5] La "firma elettronica" consiste in "dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione", distinta dalla "firma elettronica avanzata", che è una firma "connessa in maniera unica al firmatario", "idonea ad identificarlo", "creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo" e "collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati". Su queste basi, che poi sono quelle dell'articolo 2 della direttiva, l'articolo 5 stabilisce che "gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura […] posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e […] siano ammesse come prova in giudizio".

elettronica, può dunque convertirsi nell'approccio visto poc'anzi a proposito dell'indifferenza tecnologica della legge; sebbene, in realtà, ciò non sia sempre possibile. Si presti attenzione al denaro, più che alla firma, in forma elettronica: dapprima, con la D-2000/46/CE, il legislatore europeo aveva pensato all'uso di un surrogato elettronico delle monete e banconote tradizionali, sotto la supervisione di autorità finanziarie nazionali, a garanzia degli utenti. Ben presto, però, l'entrata in scena di nuove modalità di pagamento e transazioni, come PayPal (v. § 4.3.3.2), ha reso la normativa del tutto inappropriata, costringendo a passare a una nuova direttiva, ossia la D-2009/110/CE.

In terzo luogo, riguardo alla potenziale neutralità delle scelte, il legislatore può optare per una specifica (modalità d'uso relativo a una data) tecnologia, sia pure, in modo tale, che le altre tecniche o approcci tecnologici possano adattarvisi. Tornando alle firme elettroniche, il ricordato articolo 5 della D-1999/93/CE richiede ad esempio che un terzo certifichi la firma tra le parti interessate, per ciò stesso imponendo una condizione che le tecniche di firma biometrica, tra le altre, non avevano preventivato. Ciò non toglie che tali tecniche biometriche possano incorporare la figura di un terzo certificatore: analogamente, l'articolo 11(2) della direttiva europea sul commercio elettronico, ossia la D-2000/31/CE, stabilisce che "nel caso in cui il destinatario di un servizio inoltri il proprio ordine mediante strumenti tecnologici […] gli Stati membri provvedono affinché, salvo diverso accordo tra parti diverse da consumatori, il prestatore metta a disposizione del destinatario del servizio strumenti tecnici adeguati, efficaci ed accessibili tali da permettere a quest'ultimo di individuare e correggere errori di inserimento dei dati prima di inoltrare l'ordine". Sebbene, al momento dell'entrata in vigore della normativa nei primi anni 2000, poche piattaforme per l'e-commerce fossero in grado di soddisfare i requisiti della direttiva, nell'arco di pochi anni tali piattaforme sono state riadattate per ottemperare la norma.

Come ben si vede, l'approccio della neutralità tecnologica della legge non deve essere inteso come un dogma ma, piuttosto, come mezzo per disciplinare un dato campo dell'interazione degli individui, nonché gli effetti dei loro comportamenti rispetto ai quali, poi, prendere posizione sullo sviluppo e progresso del settore tecnologico.

Assunta questa prospettiva, è dunque possibile evitare gli apriorismi del dibattito, tra chi propende per una regolazione per principi o, quantomeno, formulazioni di tipo onnicomprensivo e chi, invece, sottolinea i vantaggi di una regolamentazione dettagliata e specifica della disciplina. Tanto più generale la formula delle disposizioni, tanto più esse tenderanno a sfumare e diventare vaghe, come nel caso della "neutralità di internet" che, per via della specifica complessità dell'argomento (v. § 3.4.2), stante i diversi assetti economici nell'infrastruttura della rete e dei servizi offerti agli utenti, finisce per avere differenti significati negli Stati Uniti d'America e in Europa. Si pensi ad esempio all'accordo tra Verizon e Google, nell'agosto 2010, contro una completa neutralità della rete negli Stati Uniti che, invece, Google appoggia in Europa.

Ma tanto più specifico e dettagliato il fine della regolamentazione, tanto maggiore il rischio che quest'ultima non sia in grado di tenere il passo del progresso e sviluppo tecnologico, rendendo vischioso il sistema e difficile in molti casi la sua attua-

zione. Avremo modo di vedere nei prossimi capitoli come questa sia stata, spesso, la critica a molte delle disposizioni europee in materia di tutela dei dati personali, e come tale rischio sembri addirittura accrescere con la mole di provvedimenti presentati dalla Commissione con la nuova proposta di regolamento in materia. Tra la Scilla di precetti vaghi e generali che sfumano nel vuoto, e la Cariddi di disposizioni messe facilmente fuori gioco dalla prassi, il rischio è, insomma, quello denunciato da un componente della Camera dei Lord britannica, al momento di discutere un progetto di legge [Bill] nel 2000: "Una delle tante difficoltà che ho con il Bill è che, nei suoi sforzi stridenti per essere tecnologicamente neutro, esso dà spesso l'impressione o che è ignorante sul modo in cui concretamente la tecnologia opera, oppure pretende che non ci sia affatto la tecnologia" (in Reed 2012: 201).

Torniamo, per questa via, a quel dovere di conoscenza su cui ci siamo soffermati nel capitolo terzo (§ 3.4.3.2).

Per non ripetere cose già dette, tuttavia, sarà opportuno insistere sul fatto che il fine del diritto come meta-tecnologia non è certo la soddisfazione, fine a se stessa, di regolare il progresso e lo sviluppo tecnologico. Piuttosto, si tratta di determinare come e, in molti casi, se intervenire in un determinato campo dell'interazione degli individui, al fine di disciplinarne gli effetti del comportamento che s'intrecciano con questioni di ordine tecnologico. Per poter definire la legittimità o opportunità dell'intervento, appare di qui necessario misurarsi con i valori in gioco in quel determinato settore del quale si discute. Occorre passare, cioè, all'esame della seconda variabile dell'indagine sui dilemmi posti dal design, distinguendo tra il problema di immettere nel design dei prodotti, processi, spazi o luoghi, le scelte politiche dell'intervento, e come a sua volta il design veicoli di per sé determinati valori.

### 5.3.2. *I valori in gioco*

È stato più volte sottolineato come le istanze valoriali degli individui e dei sistemi sociali rilevino per lo sviluppo della tecnologia e, soprattutto, come i conflitti tra valori e le loro diverse interpretazioni possano incidere sul design, a seconda di ciò che viene ritenuto buono o degno di protezione (si v. Flanagan, Howe e Nissenbaum 2008).

Si consideri l'esempio della tutela dei dati personali e come le diverse concezioni che possiamo avere di tale diritto – concepito, volta a volta, in termini di proprietà privata; di tutela della dignità; come controllo totale sul flusso delle informazioni; o in rapporto alle esigenze del contesto considerato – si riflettano sul modo in cui disegniamo un interfaccia o prodotto informatico. Dobbiamo adottare il modello tipico americano dell'"opt out", per cui la volontà dell'individuo si attiva soltanto per chiedere di essere escluso da quel tipo di servizio e di raccolta dei dati, oppure quel servizio commerciale con la conseguente raccolta dei dati richiede preventivamente il consenso come "opt in"?

Inoltre, si presti attenzione a ulteriori parametri della raccolta come i criteri della qualità e minimizzazione dei dati trattati, con la loro controllabilità, confidenzialità e trasparenza. Anche in questo caso, al momento di disegnare un interfaccia o prodotto informatico, è evidente che il contemperamento di tali parametri può comportare un insieme di scelte difficili. Tornando all'esempio dei sistemi informativi

per gli ospedali (v. §§ 5.1.1 e 5.2.2), i designer dovranno privilegiare l'affidabilità ed efficienza del sistema, nel tenere separati i nomi dei pazienti dai dati sul loro stato di salute e relativi trattamenti sanitari? Che ne è degli utenti, inclusi i dottori, che possono trovare tali accorgimenti del design troppo macchinosi o complicati?

Come emerge da queste pur succinte considerazioni, anche a non discutere della bontà dei valori in gioco ma soltanto del modo in cui detti valori devono essere immessi e, talvolta, bilanciati attraverso le scelte del design, sorgono non pochi problemi relativi alle scelte dei disegnatori di prodotti e sistemi informatici, di ambienti per l'interazione degli individui, dei luoghi o spazi in cui abitiamo. Di qui, come regolarsi?

Esistono fortunatamente tutta una serie di accorgimenti e metodologie con cui affrontare simili questioni. Da un lato, possiamo far ritorno a quanto detto nel capitolo primo (§ 1.4.1), a proposito del "ciclo generatore di test" messo a punto da Simon, per cui, scomponendo il design in blocchi funzionali, è dato fare emergere i modi alternativi per venire a capo dei problemi e testarli, appunto, sulla base dell'insieme dei requisiti e vincoli della progettazione del sistema. Le diverse forme in cui è possibile immettere valori, o anche scelte legislative, nel design dei prodotti, processi, spazi o luoghi, è una scelta controbilanciata da metodi empirici per la valutazione e verifica del progetto stesso. È il caso dell'uso di prototipi, test con gli utenti in ambienti controllati per verificare l'usabilità e affidabilità del disegno, oltre all'analisi e definizione dei concetti valoriali in gioco, con il metodo dell'"operazionalizzazione". Questi approcci consentono infatti di capire come il design immetta i valori in un dato sistema informativo, in un interfaccia, ecc., perché "la verifica dell'inclusione dei valori farà probabilmente leva su strategie e metodi non dissimili da quelli applicati ad altri criteri del design come la sua efficienza funzionale e usabilità" (Flanagan, Howe e Nissenbaum 2008: 348).

D'altro canto, è il legislatore stesso che può sgravare dal compito di decidere quale approccio scegliere per il design: come detto nel paragrafo precedente, ci sono casi in cui il legislatore punta su una precisa impostazione tecnologica che, necessariamente, restringe lo spettro delle scelte dei designer. All'esempio del precedente paragrafo sulle piattaforme per l'e-commerce di cui all'articolo 11(2) di D-2000/31/CE, potremmo aggiungere i limiti stabiliti dal legislatore nordamericano nel *Health Insurance Portability and Accountability Act* (HIPPA) del 1996, con cui si dettano le condizioni che devono regolare il flusso dei dati nei sistemi informativi riguardanti il settore assicurativo e ospedaliero. Si può ovviamente discutere della bontà di questo approccio che, tanto più entra nei dettagli di una determinata tecnologia e del suo design, tanto più rischia di richiedere continui aggiornamenti, o revisioni, stante lo stesso progresso tecnologico.

Ma, appunto, non è di questo che si discute in questo paragrafo: un conto sono, infatti, le decisioni politiche e le scelte valoriali incorporate in un testo di legge, altra cosa sono le scelte che occorrono per immettere tali decisioni nel design dei sistemi informativi ospedalieri, nelle piatteforme per l'e-commerce, e via dicendo. Prova ne sia l'ulteriore esempio delle centrali nucleari: un conto è la decisione politica sul se e dove costruire eventualmente detti impianti; altra faccenda è di disegnarli in modo tale che, una volta presa la decisione di costruirli, essi siano sicuri. Si tratta della progettazione delle misure di sicurezza esaminate poco sopra (§ 5.2.2), là dove la

responsabilità etica delle scelte non riguarda tanto il loro impatto sul comportamento degli individui, quanto la meticolosità tecnica e affidabilità del progetto. Nel caso delle centrali nucleari, occorre così evidenziare la probabilità degli eventi indesiderati di cui il design deve tener conto, al fine di chiarire la sequenza di possibili incidenti che possono condurre agli eventi avversi, in rapporto alla probabilità di ogni sequenza. Ecco perché gli esperti nella valutazione della probabilità dei rischi nel settore "hanno per lo più abbandonato l'idea originaria che i risultati dell'analisi probabilistica della sequenza degli eventi nei reattori nucleari dovesse essere ragionevolmente interpretata secondo il calcolo accurato delle probabilità dei vari tipi di incidenti. Piuttosto, questi calcoli sono fondamentalmente fatti per comparare diverse sequenze di eventi, al fine di identificare gli elementi critici in dette sequenze" (Doorn e Hansson 2011: 157).

Come occorso con la progettazione e costruzione di centrali nucleari, ci possono poi essere dubbi più che legittimi sulla bontà delle scelte e delle decisioni politiche, di cui i designer dovranno in séguito farsi carico. In questo modo, tuttavia, la discussione non verte più sui valori in gioco discussi nel presente paragrafo, bensì, sulla terza variabile che impegna il nostro studio sui dilemmi del design e che, a continuazione, riassumiamo con la critica kantiana alle sfide del paternalismo.

### 5.3.3. *Paternalismo*

Abbiamo più volte incontrato il pensiero di Kant nelle pagine precedenti: nel capitolo primo (§ 1.1.3), il riferimento è andato alla sua concezione del diritto come quel particolare tipo di tecnica volta a far coesistere gli arbitri individuali. Nel capitolo terzo (§ 3.3.2), è stata invece richiamata la sua opera *Per la pace perpetua*, quale punto di riferimento indiscusso per le tesi dei globalisti nel dibattito sul diritto internazionale contemporaneo, secondo un approccio che sarebbe poi stato ripreso nel capitolo quarto (§§ 4.2.2 e 4.3.2).

In questa sede, un altro scritto di Kant, ossia *Del rapporto della teoria con la pratica nel diritto pubblico* – anche conosciuto come *Contro Hobbes*, del 1793 – è particolarmente utile per chiarire la terza variabile della nostra indagine sui dilemmi del design. Per comodità espositiva, dividiamo questo paragrafo in due parti: prima, riepiloghiamo brevemente alcuni aspetti del giusnaturalismo kantiano (§ 5.3.3.1); profili che, poi, consentiranno di delucidare alcuni dei problemi più insidiosi cui va incontro l'idea di immettere le norme del sistema giuridico nei processi, prodotti o ambienti dell'interazione umana (§ 5.3.3.2).

#### 5.3.3.1. *Il giusnaturalismo di Kant*

Al modo di Hobbes (§ 2.1.2.1), di Locke (§ 3.1.1), e di Rousseau (§ 3.1.2), anche il pensiero giuridico e politico di Kant va strutturato secondo la nota scansione che porta dallo stato di natura alla società civile, per il tramite della stipulazione di un contratto sociale.

Al pari di Locke, anche per Kant esistono veri e propri diritti allo stato di natura che, in buona sostanza, possono ricondursi all'alveo del diritto privato che disciplina i rapporti tra il "mio" e il "tuo" esterno. Come si è già visto con Locke, nondi-

meno, mancano nello stato di natura i poteri di un terzo che possa sanzionare quelle regole di diritto: di qui, che occorra uscire dallo stato di natura, dove i diritti degli individui non possono che essere provvisori, per entrare in uno stato giuridico in senso proprio che renda perentori tali diritti. In altri termini, cambia la forma ma non il contenuto dei diritti in società, dato che ciò che muta è in definitiva il modo di farli valere.

A differenza di Locke, tuttavia, il postulato kantiano del diritto pubblico che obbliga a uscire dallo stato di natura per entrare in uno stato giuridico, non è frutto di un calcolo, bensì, consiste in un vero e proprio dovere categorico. È con il contratto sociale che avviene infatti il passaggio dall'uomo come essere sensibile, sottoposto alla natura e alle leggi della provvidenza, all'uomo come essere razionale sottratto a ogni dipendenza esterna. Al modo di Rousseau, il contratto sociale consiste nel deporre, tutti, la propria libertà esterna allo stato di natura, per riprenderla subito dopo come membri di un corpo comune: anche per Kant si tratta di una convenzione o, come afferma in *Contro Hobbes*, "una semplice idea della ragione, avente però una sua indubbia realtà (pratica)" (Kant ed. 1973: 68). Se, tuttavia, abbiamo visto che in Rousseau la libertà politica divorzia dalla libertà naturale degli uomini, in Kant, invece, il concetto di libertà politica è agganciato alla libertà naturale e, cioè, alla libertà negativa come non impedimento alle scelte individuali. Con le parole del filosofo tedesco, "poiché ora ogni limitazione della libertà mediante l'arbitrio di un altro è coazione, ne segue che la costituzione civile è un rapporto di uomini liberi che (fatta salva la loro libertà nel tutto della loro unione con gli altri) vivono però sotto leggi coattive; la ragione stessa così vuole, e precisamente la ragione pura, legislatrice a priori, che non ha riguardo a scopi empirici di sorta (i quali tutti sono classificati sotto il nome di felicità). Nei riguardi di tali scopi infatti, poiché ognuno li ripone in ciò che vuole, gli uomini la pensano in maniere diversissime, cosicché la loro volontà non può ricondursi ad alcun principio comune e quindi neppure ad alcuna legge esterna che si concili con la libertà di ciascuno" (Kant, *op. cit.*, 60).

Su queste basi poggia la dura critica kantiana a qualsivoglia forma di paternalismo e, cioè, all'idea che compito di chi governa, sia quello d'insegnare ai governati ciò che è buono o utile per loro, oppure, al contrario, dannoso: "nessuno può costringermi a essere felice a modo suo (nel modo cioè in cui egli [il sovrano] si immagina il benessere degli altri uomini)" (*op. cit.*, 61). La forma di governo che Kant teorizza è perciò patriottica e mai paterna, dato che spetta a ciascun essere umano decidere come vivere la propria vita. Il limite è definito dalla necessità di "difendere i propri diritti mediante leggi della volontà generale e senza ritenersi autorizzato ad usarne a suo arbitrio illimitato", per cui questo "diritto di libertà compete a lui, membro del corpo comune, in quanto uomo, in quanto cioè l'uomo è un ente capace in genere di diritti" (*ibidem*).

Nella definizione di libertà ora formulata, non sarà sfuggito al lettore il richiamo che Kant fa della nozione di volontà generale di Rousseau. Infatti, oltre alla sfera di libertà che spetta a ogni membro della società in quanto uomo, lo stato civile di Kant si fonda su due ulteriori principi a priori della ragione: quello dell'eguaglianza di ogni membro della società con ogni altro individuo, e quello dell'indipendenza di ogni membro di un corpo comune in quanto cittadino. In quest'ultimo caso, ancora una volta sulla scia di Rousseau, Kant pensa a ciascun membro del corpo comune

come partecipe del potere legislativo, ossia "una volontà pubblica da cui deriva tutto il diritto, e che quindi non deve poter fare torto a nessuno" (*op. cit.*, 65). È un'idea che, come detto, sarà sviluppata da Kant in chiave federativa e internazionale, ripresa nei secoli a venire dai teorici globalisti all'insegna dell'uomo come cittadino del mondo. Ma, che dire invece del principio di eguaglianza?

È qui, infatti, che si annidano le peggiori contraddizioni *Del rapporto della teoria con la pratica nel diritto pubblico* kantiano. Con buona pace del sottotitolo dell'opera, ossia *Contro Hobbes*, Kant segue la falsariga di un sovrano, o "capo dello Stato", come unico soggetto a non essere sottoposto alle leggi dell'ordinamento: "ché se anch'esso potesse venire costretto, non sarebbe capo dello Stato e la serie ascendente della subordinazione andrebbe all'infinito. Se poi vi fossero due di tali persone (esenti da coazione), nessuna sarebbe soggetta a leggi coattive e l'una non potrebbe fare all'altra atto ingiusto, il che è impossibile" (*op. cit.*, 62).

Vero è che, a detta di Kant, il contratto sociale si pone come un ideale regolativo che consente di stabilire quando le leggi sono, o meno, giuste; a seconda cioè di ciò su cui è possibile, o meno, prestare consenso. In ragione del contratto sociale, a ben vedere, si tratta "di obbligare ogni legislatore a far leggi come se esse avessero potuto derivare dalla volontà comune di tutto un popolo e di considerare ogni suddito, in quanto vuole essere cittadino, come se egli avesse dato il suo consenso ad una tale volontà. Questa infatti è la pietra di paragone della legittimità di ogni qualsiasi legge pubblica" (*op. cit.*, 68). Tuttavia, prosegue Kant, "se un popolo sotto una data legislazione positiva dovesse giudicare con ogni probabilità compromessa la sua felicità, cosa dovrebbe fare? Ribellarsi? La risposta può essere una sola: a quel popolo non rimane che obbedire" (*op. cit.*, 69).

Si è già visto nondimeno come, fortunatamente, i vicoli ciechi in cui va a parare in questo modo Kant, per via di un capo dello stato sovrano sottratto ai principi e norme dell'ordinamento, siano stati superati dalla costituzione dei moderni (v. § 3.1.3): in fondo, soltanto dieci anni dopo che Kant pubblica lo scritto che siamo venuti commentando in questo paragrafo, ci sarebbe stata la prima fondamentale sentenza della Corte Suprema nordamericana, sotto l'egida di John Marshall, in *Madison vs. Marbury* (§ 3.2).

Possiamo per ciò sorvolare sull'ipoteca hobbesiana, e rousseauiana, di Kant, per concentrarci invece sul legato più vivo del suo pensiero giuridico, ossia l'accennata critica alle istanze del paternalismo. Occorre mettere a frutto il suo insegnamento per misurarci con il terzo dilemma del design contemporaneo.

### 5.3.3.2. *Il disegno del paternalismo tecnologico*

Per giudicare il design giuridico odierno con Kant, dobbiamo tornare ai fini che il design stesso può avere. Rispetto alla tripartizione esaminata nel § 5.2, possiamo tuttavia tralasciare la finalità del design volto a ridurre l'impatto degli eventi dannosi, ossia le misure di sicurezza come gli airbag digitali (§§ 5.2.2 e 5.3.2). Infatti, questo tipo di design non riguarda o non incide direttamente sul comportamento degli individui ma, appunto, si concentra sull'eventualità che tale comportamento possa dar luogo a eventi dannosi, onde limitare, attenuare o neutralizzarne gli effetti.

Pertanto, possiamo concentrarci sulle due restanti finalità del design, vale a dire quella di indurre gli individui a mutare il proprio comportamento e quella di preve-

nire, tramite il design, che eventi dannosi si verifichino. Nel primo caso delle sanzioni positive (§ 5.2.1), il principio kantiano dell'autonomia individuale è fatto salvo, in tutti i casi in cui il mutamento del comportamento individuale avviene, ampliando lo spettro delle scelte messe a disposizione dell'individuo. È ciò che abbiamo visto all'opera con gli incentivi, le forme di baratto digitale, i meccanismi di reputazione e via dicendo. Si tratta in certi casi di un tipo di paternalismo che, con ossimoro volontario, è stato anche presentato come "paternalismo libertario" (Thaler e Sunstein 2009). Si pensi alla contrapposizione, ormai a noi ben nota, tra i meccanismi di "opt out" e "opt in" ma, questa volta, applicati al caso della donazione d'organi: come recita il corrispondente sito del ministero della salute italiano, "la donazione degli organi è un atto di grande civiltà e di rispetto per la vita" che è disciplinato dalla legge 91 del 1999, aggiornata dal decreto ministeriale dell'aprile 2008. La legge 91 aveva contemplato la clausola del silenzio assenso ("opt out"), che avrebbe certamente fatto accrescere di molto il numero di organi a disposizione dei medici: per una serie di ragioni politiche e culturali su cui non è caso di discutere ora, tuttavia, alla fine è prevalsa la strategia dell'"opt in", per cui, ai sensi dell'articolo 23 della legge 91, è prevista una dichiarazione di volontà a donare organi e tessuti. Nel caso in cui la legge fosse però rimasta ferma sull'impostazione originale del silenzio assenso, avrebbe potuto essere tacciata di paternalismo?

In senso stretto, a mio avviso, no; potendosi parlare, con Thaler e Sunstein, di una forma di "paternalismo soffice" e, beninteso, a condizione di una corretta campagna d'informazione pubblica. La ragione per la quale il proposito d'insegnare ai governati ciò che è buono o nobile per loro, non offende o intacca la nostra autonomia kantiana, dipende dal fatto che è pur sempre fatta salva l'opzione contraria di chiamarsi fuori (opt out).

Le cose vanno diversamente per quanto riguarda invece lo scopo del design di prevenire del tutto il fatto che eventi dannosi si verifichino: per rimanere all'esempio di prima, si pensi a quante vite umane non si salvano per mancanza di donazioni d'organi o tessuti. In questo caso, come suol dirsi, il fine giustifica i mezzi?

Ancora una volta, ma per altre ragioni, la risposta è negativa. Nello specifico del design, ci sono infatti motivi etici, giuridici e tecnici, che rendono illegittimo lo scopo di (sperare di) prevenire il verificarsi di eventi dannosi con il disegno dei processi e dei prodotti, degli spazi e dei luoghi, che mediano l'interazione degli individui. Questi motivi trascendono i profili normativi del design giuridico, per coinvolgere l'intero impianto istituzionale. Quanto ai motivi etici, infatti, si elimina del tutto la possibilità di un comportamento virtuoso perché, come insegnava Kant, si può anche costringere gli individui a comportarsi secondo ciò che la legge prescrive, ma non li si può costringere a essere buoni. Quanto ai motivi giuridici, c'è poi ampia e comprovata letteratura scientifica che evidenzia il modo in cui particolari configurazioni di valori sociali, etici o politici, siano direttamente e sistematicamente realizzati, o soppressi, dal disegno tecnologico (v. Flanagan, Howe e Nissenbaum 2008). Ciò è cruciale perché l'idea di un controllo sociale a mezzo del design mette a repentaglio l'idea stessa di stato di diritto per un triplice ordine di motivi:

i) come ricordato con Lessig più sopra (§ 5.2.3), c'è il rischio che le scelte sulle configurazioni dei valori sociali, etici o politici, siano fatte dai programmatori più che dagli individui e dalle istituzioni che eventualmente li rappresentano;

ii) anche ad ammettere che il design sia stato legittimato dal consenso popolare in un sistema giuridico, rimane la specificità della regolamentazione in rete (§ 3.4.3): nel disciplinare gli effetti extra-territoriali dell'interazione sociale, gli stati finiscono per (tentare di) imporre norme su individui che risiedono in altre zone del pianeta e che non hanno certamente avuto modo di prendere parte, sia pure mediante processi di democrazia indiretta o rappresentativa, a quelle stesse decisioni;

iii) nel sostituire con lo sviluppo e uso di "tecnologie auto-attuantesi" la tecnica del diritto tradizionale, imperniata sulla minaccia di sanzioni a supporto del comando della legge, vengono meno le garanzie e la ricchezza del momento attuativo del diritto, che tiene conto, eventualmente tramite il giudizio delle corti, delle circostanze del caso con le sue eccezioni. In altri termini, "la perfetta applicabilità [della legge] fa svanire la pubblica comprensione del diritto in quanto la sua applicazione [automatica] elimina un utile interfaccia tra i termini della legge e la sua imposizione. Parte di ciò che ci rende umani sono le scelte che facciamo ogni giorno su quel che rappresenta alcunché di giusto o sbagliato [...] In un ambiente monitorato e sorvegliato del tutto, quelle stesse scelte svaniscono" (Zittrain 2007: 152).

Come se non bastasse, ci sono infine ragioni di tipo tecnico che sconsigliano di affidarsi ciecamente al disegno di tecnologie mirate alla prevenzione totale degli eventi dannosi. Per quanto si siano sottolineati fin dal capitolo primo, gli sviluppi dell'intelligenza artificiale nel campo del diritto (§ 1.4.1), rimane la difficoltà di far sì che una macchina comprenda i concetti impiegati dai giuristi, tramite la formalizzazione di norme, diritti o doveri: di questo passo, "non solo è inevitabile il rischio di fallimenti operativi, ma la finalità di disegnare standard che siano in grado di raggiungere l'obiettivo desiderato dal regolatore in forma precisa e accurata, non può che essere, con ogni evenienza, un'impresa improba" (Yeung 2007: 106).

Eppure, come riferito più sopra (§ 5.2.3), la produzione e uso di tecnologie volte all'applicazione automatica della legge ha avuto e gode tuttora di grande popolarità, non solo in alcuni ordinamenti dove, in fondo, la cosa non sorprende, come in Cina, ma anche in Occidente. In fondo, l'idea è di risolvere per questa via, altrimenti intrattabili problemi riguardanti l'efficacia delle leggi in internet, conflitti di competenza e giurisdizione, oltre a questioni inerenti alla sicurezza nazionale, la lotta al cyber-terrorismo e la pedo-pornografia in rete. Stante la serietà dei problemi posti a legittimazione del "controllo totale" tramite design, vale la pena di approfondire a parte questi temi, nel prosieguo del capitolo.

## 5.4. *L'applicazione automatica della legge*

L'intento di rendere automatica l'applicazione della legge tramite il disegno di tecnologie auto-attuantesi, quali sistemi onnipervasivi di filtraggio, tecniche DRM a tutela della proprietà intellettuale o certe versioni della "privacy tramite design" (Cavoukian 2010), riporta la nostra attenzione alla tavola 6 del capitolo quarto (§ 4.3.3.2).

In quel contesto, l'accento era posto sulle spinte centrifughe e centripete cui è sottoposto l'antico monopolista delle fonti nel modello di Westfalia, ossia il guber-

naculum del diritto nazionale come primo osservabile della tavola 6. Il precedente capitolo, non a caso, si è chiuso con un paragrafo che s'interroga su un diritto senza o contro lo stato.

Qui, per converso, l'accento cade sulla spinta eguale e contraria che, facendo leva sull'uso della tecnologia al fine di pervenire a una applicazione automatica della legge, finirebbe per ricondurre al gubernaculum come centro delle fonti e del sistema normativo. Avendo peraltro sottolineato come la redistribuzione del sistema delle fonti si intrecci a questioni di potere (§§ 4, 4.3, 4.3.2.1, 4.3.3.3), non deve sorprendere che l'antico monopolista delle fonti tenti di riappropriarsi per via tecnologica, di ciò che la rivoluzione tecnologica ha contribuito a sottrargli.

Il nuovo controllo che è reso possibile sul comportamento degli individui, non contrasta però, necessariamente, con le altre componenti del sistema. Prova ne sia l'uso delle tecniche DRM da parte di società private a tutela dei propri diritti di copyright, che possono a loro volta essere concepite come attuazione della normativa adottata dagli stati, sia sul piano nazionale sia internazionale, e sia pure sotto gli auspici e pressione di quelle stesse società private: in fondo, i DRM sono tutelati da una specifica disposizione del trattato WIPO sul copyright introdotto già nel capitolo primo (§ 1.4.2). L'articolo 11, incentrato sugli obblighi in materia di misure tecnologiche, non a caso recita che "le Parti contraenti prevedono un'adeguata tutela giuridica e precostituiscono mezzi di ricorso efficaci contro l'elusione delle misure tecnologiche utilizzate dagli autori nell'esercizio dei diritti contemplati dal presente trattato [...] allo scopo di impedire che vengano commessi, nei confronti delle loro opere, atti non autorizzati dagli autori stessi o vietati per legge".

Dalla canonica formula "se A, allora B", si passa così dall'insieme di disposizioni normative supportate dalla minaccia di sanzioni fisiche sul piano del dover essere, a una serie di misure coattive che seguono in automatico sul piano dell'essere. Non si tratta più di influire sul comportamento individuale ma, piuttosto, di determinarlo a priori tramite il design dei prodotti, processi o ambienti dell'interazione umana, per prevenire il verificarsi di eventi dannosi. Come detto, rimangono tuttavia aperti in questo modo tre ordini di questioni. Essi riguardano se l'applicazione automatica della legge sia desiderabile, se tecnicamente fattibile e, soprattutto, sul piano istituzionale, se essa sia legittima alla luce dei principi e norme del costituzionalismo moderno.

A ciascun tipo di problema dedichiamo un paragrafo nelle pagine che seguono.

### 5.4.1. *Desiderabilità*

Dopo la critica kantiana del paternalismo, può sembrare bizzarro occuparci della desiderabilità di un controllo totale da attuarsi per il tramite del design. Basterebbe però citare i casi, cui ho fatto prima cenno, del cyber-terrorismo e della pedopornografia, per rendersi conto del problema: chi non vorrebbe prevenire del tutto questi casi efferati con l'uso di tecnologie auto-attuantesi?

A rigore, non sarebbe nemmeno il caso di parlare di paternalismo ma, bensì, della repressione o prevenzione di comportamenti malvagi, rispetto ai quali vale l'argomento kantiano della volontà generale come limite all'"arbitrio illimitato" dei singoli, con il test del consenso (§ 5.3.3.1).

Eppure, per venire sin d'ora al punto dolente che propone la questione, osta alla desiderabilità del controllo totale per il tramite del design, anche nei casi particolari del cyber-terrorismo o della pedo-pornografia su internet, i limiti tecnici di simile progetto tecnologico. Infatti, stante la natura fortemente decentrata e aperta della rete, non è dato condurre un monitoraggio specifico e, per così dire, chirurgico di queste attività illecite e, anzi, identificarne i responsabili richiede spesso un lavoro immane.

Di qui un preoccupante dilemma:

– o si smantella la rete, quale l'abbiamo finora conosciuta e come hanno fatto del resto in Cina con la "grande muraglia di fuoco" (§ 5.2.3); ma allora, come suol dirsi, butteremmo il bambino con l'acqua sporca;

– oppure si provvede a un monitoraggio indiscriminato per il tramite di filtri onnipervasivi che rimettono però in discussione la desiderabilità dell'intero progetto: infatti, non si avrebbe a che fare tanto con una deriva paternalistica, quanto autoritaria, dell'intervento che sposta il rischio dell'"arbitrio illimitato" dai singoli al gubernaculum.

Senza addentrarci sin d'ora sui profili di legalità di quest'ultimo scenario, vale la pena di illustrare per intanto i termini del problema con l'immagine di un'autostrada: al pari d'internet, anche alle autostrade si applica il principio che l'intelligenza è posta agli estremi della rete, nel senso che rappresentano un mezzo affinché gli individui possano raggiungere i fini più vari. Del pari, come occorre per internet, anche le autostrade possono essere utilizzate per fini illeciti, come il trasporto di droghe o armi; tuttavia, anche in quest'ultimo caso, quantomeno nei paesi occidentali, tale eventualità non giustifica un sistematico controllo generalizzato della rete (sia autostradale sia d'internet). A riprova, basti pensare che questo controllo sistematico riporterebbe ai viaggi in macchina verso Berlino ovest prima della caduta del Muro (1989), e al modo in cui le autostrade erano gestite a quei tempi dall'allora Germania dell'est (DDR); vale a dire, con i paranoici controlli di polizia a tutto spiano e il filo spinato a isolare le corsie stradali. È questo che vogliamo?

### 5.4.2. *Fattibilità*

A prescindere dall'ambito di ciò che reputiamo desiderabile, o meno, c'è lo spazio di ciò che si può concretamente fare stante i rapporti di forza e le variabili da considerare in un contesto determinato. Tornando agli osservabili della tavola 6 nel capitolo quarto (§ 4.3.3.2), l'intento di prevenire gli eventi dannosi del comportamento individuale tramite un controllo totale a mezzo del design, si scontra con le altre modalità regolative di tale comportamento. Rimandando al prossimo paragrafo il ruolo che la iurisdictio svolge in questo contesto, concentriamoci per intanto sulle norme sociali del kosmos e le forze del mercato, sulla base di due punti principali.

Innanzitutto, l'impiego del design per prevenire il verificarsi di eventi dannosi o i comportamenti indesiderati degli individui, vanta una tradizione più che ventennale nel settore privato. Avendo presente che le modalità tecniche di come funzioni il design, in fondo, rimangono le stesse, indipendentemente cioè dal fatto di che le ponga in essere, questa esperienza privata del design ai fini del controllo totale risul-

ta dunque istruttiva anche per il settore pubblico. A conferma di quanto detto sulla vulnerabilità di questi progetti (si v. §§ 5.3.3.2 e 5.2.3, a proposito della falla nella "grande muraglia di fuoco" cinese nel gennaio 2014), la fattibilità di simili programmi è stata infatti messa a dura prova anche per quanto riguarda il suo terreno d'origine, il settore privato. Sul piano pratico, si può essere quasi certi che per ogni dispositivo volto al controllo del comportamento umano, di lì a poco sarà messo a disposizione il contro-dispositivo.

Emblematico il caso della tecnologia CSS con cui, nel 1996, l'industria del DVD aveva pensato di tutelare i propri diritti, impedendo la copia digitale di tali prodotti. Con buona pace dell'articolo 11 del trattato WIPO sul copyright ricordato poco fa, tre anni dopo, nel 1999, l'antidoto al CSS, il contro-codice DeCSS era già bello che pronto. Sebbene, in teoria, l'industria del DVD avrebbe potuto reagire, creando a sua volta un De-DeCSS, pragmaticamente vi ha rinunciato, dato che avrebbe finito per danneggiare se stessa, mettendo fuori uso i lettori e supporti DVD in commercio e, per ciò, riducendo le vendite dei dischi sul mercato. Analogo discorso è valso per il sistema DRM dell'Apple Fairplay (2003) e dei contro-dispositivi anti-Fairplay che si sono succeduti a ogni nuova generazione della tecnologia iTunes; al punto tale che, il 6 febbraio 2007, nel famoso discorso sui *Pensieri sulla musica*, uno che di design s'intendeva, Steve Jobs (1955-2011), dichiarava la fine di Fairplay e delle restrizioni per le copie digitali di iTunes: "i DRM non hanno funzionato e potrebbero non funzionare mai per fermare la pirateria musicale" (Jobs 2007). Insomma, anche nei settori in cui l'applicazione automatica delle regole sembra più facile o alla portata dei programmatori, come nel caso del copyright, si può ripetere quanto detto nel capitolo primo (§ 1.4.1), per cui neanche a mettere un sistema informatico "dentro a un blocco di cemento e sigillato a piombo in una stanza attorniata da guardie giurate", potrebbe renderlo del tutto sicuro (Garfinkel e Spafford 1997: 9).

La difficoltà, per non dire l'impossibilità tecnica di garantire l'efficienza del design a controllo totale, introduce in questo modo il secondo punto al quale occorre prestare attenzione. Come detto (§ 4.3.1.1), le norme del diritto non operano in una sorta di vuoto pneumatico, ma concernono le pratiche sociali di una comunità che, spesso, va in controtendenza (o si oppone chiaramente) alle modalità di controllo totale del design: è il caso delle proteste portate avanti dagli utenti di Facebook (§ 5.1.3), o delle sanzioni positive di eBay e nei sistemi P2P (§ 5.2.1), cui possiamo qui aggiungere il caso dei cookie (§ 4.3.3.1). Inizialmente sviluppati dagli informatici per risolvere una serie di problemi tecnici, i cookie vennero impiegati dai fornitori di servizi per il commercio elettronico per agevolare idealmente i propri servizi. Tuttavia, davanti alle proteste dei consumatori e dei gruppi a tutela della privacy, gli informatici sono corsi ai ripari, modificando la tecnologia per venire incontro a quelle proteste e "questo è successo senza alcuna minaccia legale e contro l'ovvia razionalità economica" (Mayer-Schönberger 2008: 743).

La lezione da trarre sulla fattibilità del disegno di una legge ad applicazione automatica è dunque chiara: o l'intento del gubernaculum di avvalersi di tecnologie auto-attuantesi trova corrispondenza nelle norme sociali del kosmos e nel mercato, oppure il disegno è destinato a vita breve. Ciò dipende, in certi casi, dalle contromisure tecnologiche che troveranno terreno fertile tra i membri della comunità, altre volte per via della concorrenza e orientamenti diversi tra gli attori del mercato –

come nel caso di scuola nordamericano tra la *west coast economy* votata al digitale e l'*east coast economy* ispirata ai modelli del business tradizionale – su cui andranno poi a inserirsi o far leva le dinamiche del kosmos. Di qui, che "al posto di un flusso unidirezionale di comunicazioni coercitive, troviamo invece un complesso intreccio d'interazioni tra i singoli utenti del cyberspazio, produttori di codici, legislatori e mercati. Comunicazione e retroazione comportano nell'insieme uno sviluppo evolutivo della tecnologia, piuttosto che determinarne l'aspetto come il risultato che proviene da una più alta autorità (come i mercati o la legge)" (Reed 2012: 209).

Beninteso, ciò non significa che il legislatore debba smettere di fare le leggi o che debba semplicemente seguire ciò che dettano il mercato o le norme sociali della comunità. I limiti alla fattibilità del design che aspira al controllo sociale, piuttosto, riconducono ai criteri normativi introdotti nel capitolo terzo e, in particolare, sia al dovere di conoscenza (§ 3.4.3.2), sia alla scelta degli strumenti da impiegare (§ 3.4.3.3).

A volte, si dovrà ricorrere alle sanzioni positive del design oppure, come nel caso della lotta alla pedo-pornografia con cui siamo partiti nel paragrafo precedente, a forme di collaborazione con i fornitori di servizi in rete ed enti come l'*Internet Watch Foundation*, per stilare la lista dei siti da bloccare.

Altre volte, però, sarà opportuno valersi ancora del consueto apparato repressivo della legge, supportato da sanzioni fisiche, purché, come detto (§§ 5.3.1 e 5.3.3.2 (b)), precisando la comunità dei destinatari dell'intervento nel caso della interazione in rete e chiarendo le intenzioni ed effetti del loro comportamento, ritenuti giuridicamente rilevanti al fine di definire lo scopo della legge.

In ogni caso, rimane determinante il ruolo che i principi del sistema svolgono nel delimitare le scelte del legislatore; ciò che riconduce al piano della iurisdictio evidenziato fin dal capitolo terzo (§ 3.2). Dopo la desiderabilità e fattibilità del design volto ai fini del controllo totale, nel rapporto tra gubernaculum, mercato e kosmos, occorre indagarne a continuazione il piano della legalità.

### 5.4.3. *Legalità*

Nonostante la nutrita schiera di ragioni che ostano all'uso del design a controllo totale, abbiamo detto dei numerosi tentativi di avvalersene per approdare all'applicazione automatica della legge. La tentazione, del resto, è grande se, d'un colpo solo, fossimo in grado di risolvere non solo gravosi problemi di competenza e giurisdizione, ma anche di garantire il rispetto della legge in ossequio al principio di certezza del diritto!

Ma, stanno proprio così le cose?

Istruttive sono, al riguardo, due sentenze della Corte di giustizia europea nei casi *Scarlet Extended* (C-70/10) e *Netlog* (C-360/10). In entrambi i casi l'attore è stato la SABAM – corrispondente alla SIAE italiana – che rappresenta gli autori, compositori ed editori di opere musicali in Belgio. La SABAM è l'ente che autorizza l'uso da parte di terzi, delle opere musicali protette dal copyright di quegli autori, compositori ed editori, per cui, nel giugno 2009, veniva presentato un ricorso davanti alla Corte di prima istanza a Bruxelles: prima un fornitore di servizi in rete, e cioè Scarlet, poi una piattaforma sociale, e cioè Netlog, avrebbero infatti reso dette opere disponibili al pubblico senza l'autorizzazione dell'attore, e senza pagargli alcun corrispettivo.

Più in particolare, la SABAM richiedeva ai giudici di ingiungere ai convenuti di prendere le misure appropriate per porre fine a tutte le violazioni della proprietà intellettuale fatta valere dall'attore, e allo scopo di prevenire qualsiasi ulteriore violazione in futuro. Nel caso di Netlog, la Corte di Bruxelles avrebbe quindi dovuto ingiungere alla piattaforma sociale di installare un sistema che, con le parole della Corte di Lussemburgo, avrebbe dovuto filtrare:

a) "L'informazione che è conservata sui suoi server da parte degli utenti del servizio;
b) che si applica indiscriminatamente a tutti quegli utenti;
c) come misura preventiva;
d) esclusivamente a spese di Netlog; e
e) per un periodo illimitato;
che è in grado d'identificare i file elettronici contenenti opere musicali, cinematografiche o audio-visive, rispetto alle quali chi chiede l'ingiunzione [SABAM] rivendica diritti di proprietà intellettuale" (C-360/10, § 53).

Il 16 febbraio 2012, la Corte di giustizia ha tuttavia stabilito che questo sistema di filtraggio è incompatibile con le direttive sul commercio elettronico (2000/31/CE), sul copyright (2001/29/CE), sulla proprietà intellettuale (2004/48/CE), sulla protezione dei dati (1995/46/CE), e la libertà di ricevere o dare informazione, ai sensi degli articoli 8 e 11 della Carta UE dei diritti fondamentali. "Per di più, tale ingiunzione [d'installare i sistemi di filtraggio] è potenzialmente in grado di danneggiare la libertà d'informazione, in quanto tale sistema potrebbe non distinguere adeguatamente tra contenuto lecito e contenuto illecito, con il risultato che la sua introduzione potrebbe condurre al blocco di comunicazioni lecite" (§ 50 della decisione).

Inoltre, richiamando i propri precedenti – in particolare: C-275/06, ossia il caso *Promusicae* – la Corte ha dichiarato che nessuno dei diritti di proprietà intellettuale può ritenersi "inviolabile" o "assoluto" ma, piuttosto, che questi diritti vanno bilanciati con la tutela degli altri diritti fondamentali previsti dall'ordinamento. Tuttavia, è da notare che nessun bilanciamento si è reso necessario nel caso Netlog: infatti, ancora una volta con le parole della Corte, il diritto europeo "deve essere interpretato in modo da precludere che una corte nazionale possa ingiungere a un fornitore di servizi hosting d'installare un sistema di filtraggio", come quello descritto sopra. L'idea stessa di provvedere per il suo tramite a una applicazione automatica della legge è, in altri termini, illegittima.

Nondimeno, a prevenire conclusioni affrettate, c'è da aggiungere quanto occorso nel Regno Unito poco dopo la sentenza ora citata, a proposito del sistema di filtraggio previsto dal *Digital Economy Act* (DEA), già richiamato sopra (§ 5.2.3). In sostanza, la legge britannica prevede un "codice di obbligazioni" che dovrebbe imporre ai fornitori di servizi in rete (ISP) sia il compito di notificare agli utenti sospetti di violazione di copyright i rapporti stilati dai detentori di tali diritti, sia di fornire a questi ultimi le liste di violazioni di copyright, oltre a una serie di "obbligazioni tecniche" incluse in un "codice". Alcuni ISP, come British Telecom, hanno tuttavia eccepito la violazione del diritto europeo in tema di tutela dei dati personali, comunicazioni elettroniche e libertà d'impresa, richiamandosi in forma espressa ai precedenti della Corte di giustizia nei ricordati casi *Promusicae* e *Scarlet*. Finita la

controversia davanti ai tribunali, tanto in primo, quanto in secondo grado, i giudici britannici si sono pronunciati per la legittimità delle disposizioni approvate dal Parlamento di Westminster. Con le parole della Corte d'appello di Londra, il 6 marzo 2012, "una certa quantità di energia è stata spesa davanti a noi sul recente giudizio della Corte di Giustizia in *Scarlet* […] concernente la compatibilità con la direttiva sulla privacy e le comunicazioni elettroniche e con altre direttive circa l'ingiunzione di una corte di imporre a un ISP d'installare un sistema per filtrare le comunicazioni elettroniche, al fine di identificare e bloccare il trasferimento di file che violino il copyright. Sia l'Avvocato generale sia la Corte hanno citato *Promusicae*, in termini tali che, a mio avviso, non chiariscono granché il senso di tale decisione; ma io non vedo nulla nel caso che supporti lo scopo limitato che gli attori cercano di dare alla decisione in *Promusicae*" (CI/2011/1437, n. 82).

Sulla base di questa pronuncia può comprendersi perché, come detto, tra il 2013 e il 2014, il governo britannico sia tornato alla carica, implementando un sistema di filtri per prevenire la visita dei siti pornografici in rete (§ 5.2.3). Significativamente, il sistema ha cominciato a bloccare siti altamente pericolosi come quello di Amnesty International, l'Electronic Frontier Foundation (eff.org), il sito del gruppo degli utenti Unix, e molto altro ancora!

Dal punto di vista giuridico, qualora i giudici britannici dovessero mai convincersi dell'opportunità di ricorrere in via pregiudiziale alla Corte di giustizia (§ 4.3.2.1 (d)), per capire il senso da dare alle sue decisioni in *Promusicae*, *Scarlet*, e *Netlog*, è più che probabile che questi sistemi di filtraggio saranno ritenuti anch'essi incompatibili con i principi del diritto europeo, "non distinguendo adeguatamente tra contenuto lecito e illecito" delle comunicazioni (§ 50 della decisione in *Netlog*).

Ma, che dire nel caso in cui la posta in gioco non sia già la lotta alla pornografia in rete, ma la stessa sicurezza nazionale?

In questo caso, infatti, non possiamo fare riferimento alla giurisprudenza della Corte di Lussemburgo, perché priva di competenza generale; ma, piuttosto, alle Corti nazionali e in ultima istanza, per rimanere in Europa, alla Corte di Strasburgo per la tutela dei diritti umani o CEDU. Sebbene non si siano ancora discussi casi del genere davanti a quest'ultima corte, c'è tuttavia da pensare, in ragione dei suoi precedenti, che neanche in questo caso sarebbe legittimo l'uso di un sistema onnipervasivo e indiscriminato di filtri. Si pensi a com'è stato interpretato il combinato disposto dei due commi dell'articolo 8 della Convenzione europea dei diritti dell'uomo, per cui "non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto [al rispetto della vita privata e familiare, del proprio domicilio e della corrispondenza] a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza […] alla difesa dell'ordine e alla prevenzione dei reati". Così, la nozione di "necessità" è stata interpretata nel senso di un "impellente bisogno sociale" (si v. il caso *Gillow vs. Regno Unito*, deciso il 24 novembre 1986, § 55), per cui "le autorità nazionali godono di un margine di apprezzamento, il cui scopo dipenderà non solo dalla natura del legittimo scopo perseguito ma anche dalla particolare natura dell'interferenza prodotta" (caso *Leander vs. Svezia* del 26 marzo 1987, § 59). Ad esempio, nel controllare segretamente la corrispondenza e telecomunicazioni dei cittadini allo scopo di combattere il terrorismo, la Corte ha segnalato che la necessi-

tà di un "certo compromesso tra le esigenze di difendere la società democratica e i diritti delle persone è implicito nel sistema della Convenzione" (in *Klass e altri vs. Germania* del 6 settembre 1978, § 59). Insomma, senza dover ripercorrere tutta la casistica della Corte di Strasburgo, è abbastanza pacifico che qualsiasi sistema di filtraggio ai fini della sicurezza nazionale o dell'ordine pubblico, non possa essere indiscriminato; ma, debba prevedere qualche forma di bilanciamento o contemperamento dei diritti e interessi in gioco.

A conferma dell'assunto, si presti poi attenzione alla proposta di direttiva che la Commissione europea ha presentato nel gennaio 2012, per la protezione dei dati personali nel settore delle attività di polizia e la giustizia penale. Al punto 38 della proposta, si legge che "la protezione dei diritti e delle libertà degli individui in rapporto al trattamento dei dati personali, richiede che siano prese misure tecniche e organizzative appropriate, per garantire che i requisiti della direttiva siano soddisfatti. Al fine di garantire l'ottemperanza delle disposizioni adottate ai sensi di questa direttiva, il responsabile [dei dati personali] dovrà adottare politiche e implementare misure appropriate che soddisfino in particolare i principi della tutela dei dati tramite il design e come assetto base della configurazione dei sistemi informativi". Ai sensi dell'articolo 16 TFUE, la Commissione ricorda inoltre che la direttiva è tenuta a rispettare il principio di sussidiarietà (v. § 3.3); per cui il senso dell'intervento della direttiva va commisurato, in sostanza, a quanto strettamente necessario e là dove i suoi obiettivi, per motivi di scala o degli effetti dell'azione, non possano essere raggiunti dai singoli stati membri. Infine, è rimarchevole che il settimo considerando della proposta di direttiva faccia riferimento a "un livello di protezione dei diritti e libertà degli individui in rapporto al trattamento dei dati personali da parte delle autorità competenti ai fini della prevenzione, investigazione, rilevamento e persecuzione delle offese penali o di esecuzione delle condanne penali" che "deve essere equivalente in tutti gli stati membri".

Anche a trovare conforto nella tesi che qui si sostiene con la giurisprudenza delle Corti di Strasburgo e Lussemburgo, nonché con la direttiva proposta dalla Commissione europea nel settore delle attività di polizia e della giustizia penale, bisogna però ammettere che rimangono ulteriori problemi aperti. Uno su tutti: lo scandalo del 2013 sul progetto Prisma dell'Agenzia nordamericana per la sicurezza nazionale (NSA) e i cosiddetti file GCHQ britannici[6], che, grazie alle rivelazioni di Edward Snowden (n. 1983), hanno fatto capire al mondo i rischi che corriamo sul piano della tutela dei diritti costituzionali.

Per certi versi, purtroppo, si può dire che nulla di nuovo appare sotto il sole, se è vero che un sistema d'intercettazione globale delle comunicazioni era già stato messo a punto fin dal 1947 dagli Stati Uniti d'America con il Regno Unito, il Canada, l'Australia e la Nuova Zelanda, e di cui si è solo in parte saputo qualcosa a proposito del sistema di intelligenza sui "segnali" noto come *Echelon*[7].

---

[6] Si v. l'articolo di John Lanchester, *The Snowden files: why the British public should be worried about GCHQ*, in "The Guardian", 3 ottobre 2013, disponibile su *http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester* (ultimo accesso il 10 settembre 2014).

[7] Sul punto rimando all'esauriente articolo di Steven Wright (2005), che è stato, peraltro, uno degli studiosi che ha contribuito a far emergere (e dibattere perfino dal Parlamento europeo) il sistema d'in-

Inoltre, si tratta di un modo ulteriore, ancorché doloroso, per ribadire ciò su cui è stata posta la nostra attenzione fin dal primo capitolo di questo libro, vale a dire come le tradizionali frontiere giuridiche e politiche degli stati evaporino nel nuovo contesto delle società ICT-dipendenti, e come l'intervento normativo dei legislatori – in questo caso, quello "garantista" dell'Unione europea – sia destinato a essere inefficace e, per così dire, spiazzato nei confronti delle tecniche di monitoraggio massiccio e indiscriminato da parte di altri stati (v. § 1.4.3).

Ad onor del vero, nel momento di scrivere queste righe, non sono mancate le prime reazioni della iurisdictio, sia pure contrastanti: mentre alcune corti nordamericane hanno dichiarato legittimo e, dunque, compatibile con la tutela degli emendamenti alla costituzione, il progetto Prisma dell'NSA, altri giudici si sono espressi in modo opposto. Basti qui riprendere le conclusioni dell'Opinione formulata dalla Corte distrettuale della Columbia, il 16 dicembre 2013, nel caso *Klayman vs. Obama*. Con le parole del giudice Richard J. Leon, "questo caso non è che l'ultimo capitolo della continua sfida della iurisdictio (*Judiciary*), per bilanciare gli interessi nazionali alla sicurezza degli Stati Uniti con le libertà individuali dei nostri cittadini. Il Governo, nel suo comprensibile zelo per proteggere la patria, ha messo a punto un programma di contro-terrorismo con rispetto ai metadati telefonici che mira a un bilanciamento in larga parte basato su un precedente più che trentennale della Corte suprema [8], la cui rilevanza è stata eclissata dallo sviluppo della tecnologia e di uno stile di vita imperniato sull'uso dei telefoni cellulari allora del tutto inconcepibile. Nei mesi a venire, non c'è dubbio che altri Corti come questa, saranno impegnate a trovare il bilanciamento opportuno ai sensi del nostro sistema costituzionale. Ma, nel frattempo, per le ragioni esposte prima, accolgo le richieste d'ingiunzione di Larry Klayman e Charles Strange, per avere un ordine che (1) vieta al Governo di raccogliere come parte del programma di metadati telefonici dell'NSA, ogni metadato telefonico dei loro contratti con la Verizon e (2) richiede al Governo di distruggere ogni metadato del genere in suo possesso, raccolto attraverso detto programma. Tuttavia, alla luce dei rilevanti interessi per la sicurezza nazionale che sono in gioco in questo caso e la novità delle questioni costituzionali, sospendo il mio ordine nell'attesa dell'appello. Facendo così, do pertanto un equo avviso al Governo che, dovesse il mio ordine essere confermato, esso sarà esecutivo immediatamente. Pertanto, sono convinto che durante il processo d'appello, che richiederà almeno il trascorso dei prossimi sei mesi, il Governo prenderà tutte le misure necessarie per prepararsi ad attenersi a questa decisione quando, e se, sarà confermata. Non c'è bisogno di dire che, nel caso si dovesse chiedere ulteriore tempo per attenersi a questa decisione, tra alcuni mesi da adesso, ciò non sarà il benvenuto e potrebbe comportare ulteriori sanzioni" [9].

---

tercettazione. I "segnali" cui si rinvia nel testo, non riguardano soltanto i messaggi trasmessi via satellite, ma anche a microonde e attraverso cavi a fibra ottica. Basti dire che, nello studiare il caso, Steven si è ritrovato un giorno i servizi segreti britannici a perquisirgli la casa all'alba …

[8] Il giudice Richard Leon fa riferimento a *Smith vs. Maryland* del 1979, su cui sotto § 7.2.4.

[9] Caso 1:13-cv-00851-RJL, doc. 48, pp. 66-68 della decisione del giudice distrettuale per la Columbia, Richard J. Leon.

## 5.5. *Un caso di scuola*

Nel corso delle pagine precedenti si è insistito sui fenomeni di complessità indotti dalla "quarta rivoluzione", esaminando il passaggio che ha condotto, da un lato, dalle forme tradizionali di governo all'odierno reticolo istituzionale della governance e, dall'altro, sul piano delle fonti, dal modello di Westfalia all'assetto policentrico e pluralistico dei diritti nazionale, internazionale e transnazionale nelle attuali società ICT-dipendenti.

Il quadro è stato poi arricchito dall'esame del design giuridico con i diversi fini che possono caratterizzare l'immissione delle regole del diritto negli ambienti, spazi o oggetti che mediano l'interazione individuale, con le relative ricadute istituzionali. Di pari passo con la descrizione di tali trasformazioni, sul piano generale, l'attenzione si è soffermata sui problemi che assillano gli ordinamenti giuridici con le questioni di trasparenza e rappresentanza della governance contemporanea, le spinte centrifughe e centripete cui è sottoposto il diritto nazionale, le tendenze del diritto transnazionale oltre, ma anche contro lo stato, fino alle questioni specifiche di internet con l'inefficacia crescente del tradizionale apparato repressivo del diritto fondato sulla minaccia di sanzioni, per via del flusso delle informazioni che trascende più spesso le canoniche frontiere degli stati. Ciò ha condotto all'idea di avvalersi dei meccanismi di tecnologie auto-applicantisi al fine di affrontare molti di questi problemi, mettendo a repentaglio alcuni capisaldi dello stato di diritto e del legato costituzionale moderno.

Con l'intento di chiarire sia il significato di queste trasformazioni, sia la portata dei problemi in atto, il lettore avrà notato quanto spesso abbiamo fatto ricorso agli esempi del settore della privacy e della tutela dei dati personali.

Nel primo capitolo, il richiamo è servito a illustrare due punti chiave dell'indagine, e cioè come la rivoluzione tecnologica abbia contribuito a riplasmare vecchi istituti (§ 1.4.2), e come la crescente inefficacia dell'intervento del legislatore in rete, testimoniata dal caso dello spamming o posta indesiderata, abbia consigliato il ricorso all'uso della tecnologia, specialmente la cosiddetta "privacy tramite design", per porre rimedio a quella stessa inefficacia (§ 1.4.3).

Nel capitolo terzo, ci si è invece soffermati sul caso Lindqvist e l'articolo 25 della direttiva europea (95/46/CE), per evidenziare come il flusso delle informazioni in rete travalichi i tradizionali confini giuridici degli ordinamenti su base territoriale, sollevando problemi rispetto ai quali è emerso il ruolo che la giurisprudenza svolge come fattore produttivo del sistema giuridico (§ 3.4.1).

Nel capitolo quarto, le norme sul trattamento e la protezione dei dati personali hanno messo in luce il ruolo che le autorità garanti e i codici di auto-regolamentazione svolgono negli ordinamenti nazionali (§ 4.3.1), oltre alle caratteristiche del cosiddetto diritto soffice (§ 4.3.1.1), e i criteri per dirimere i conflitti di competenza e giurisdizione, come nel caso dell'articolo 4 di D-95/46/CE (§ 4.3.3.1).

Infine, in questo capitolo, riprendendo lo spunto del capitolo primo sulla privacy tramite design, ci si è serviti del suo esempio per approfondire sia i temi del design dei prodotti (§ 5.1.1), sia dei messaggi, come nel caso di Facebook (§ 5.1.3), con le ulteriori questioni sul concetto di neutralità tecnologica del diritto in rapporto alla nozione di trattamento (§ 5.3.1), i valori in gioco nella contrapposizione tra

opt in e opt out (§ 5.3.2), fino ai nodi del bilanciamento dei diritti tra privacy, appunto, sicurezza e dati personali (§ 5.4.3).

Una delle ragioni principali per le quali il rimando ai temi della privacy appare così cruciale, è stata spiegata efficacemente dalla prima autorità italiana per il trattamento e la tutela dei dati personali, Stefano Rodotà (n. 1933). Legata indissolubilmente alla tutela della persona umana, la centralità dell'istituto dipende da una radicale motivazione di tipo filosofico, in quanto, spiega il giurista italiano nella *Intervista su privacy e libertà*, "la privacy si presenta come un elemento fondamentale della 'società dell'eguaglianza' […] una condizione essenziale per essere inclusi nella 'società della partecipazione' […] uno strumento necessario per salvaguardare la 'società della libertà' […] una componente ineliminabile della 'società della dignità'" (Rodotà 2005: 149).

Come emerso tuttavia nelle pagine precedenti e, sempre più chiaramente, apparirà nei prossimi capitoli, è proprio questo ruolo della privacy nella società della eguaglianza e partecipazione, della libertà e dignità, a essere stato più volte messo alla prova negli ultimi anni. Per molti aspetti, l'istituto appare infatti un caso di scuola con cui intendere tanto il riposizionamento tecnologico del diritto nell'era delle società ICT-dipendenti, quanto i problemi attinenti alla sicurezza nazionale e all'ordine pubblico, con cui abbiamo concluso il paragrafo precedente. Avendo sin d'ora a mente il test ideato dalla Corte suprema di Washington sulla ragionevole aspettativa di privacy nel caso Katz del 1967, passiamo dunque a esaminare il prossimo osservabile della nostra analisi; ossia, appunto, il fondamentale diritto alla privacy.

# Parte Speciale
## *Il test di Katz tra America ed Europa*

# VI.
# *Privacy*

> "Una vita spesa interamente in pubblico, alla presenza degli altri, diventa, potremmo dire, piatta. Pur mantenendo la sua visibilità, tale vita perderebbe la qualità di darsi allo sguardo, provenendo da un luogo più scuro che deve rimanere nascosto se non gli si vuole far perdere la profondità in un senso autenticamente reale, non soggettivo"
>
> Hannah ARENDT

Il diritto alla privacy è stato solennemente riconosciuto con la Dichiarazione universale dei diritti dell'uomo (1948), all'articolo 12: "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".

Due anni più tardi, tale diritto è stato del pari riconosciuto dalla Convenzione europea dei diritti dell'uomo (1950), all'articolo 8. Mentre il primo comma riprende quasi alla lettera la Dichiarazione universale, per cui "ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza", il secondo comma dell'articolo statuisce i limiti all'intervento dell'autorità pubblica. Come riferito sopra (§ 5.4.3), "tale ingerenza" deve essere prevista dalla legge e risultare necessaria ai fini di garantire la sicurezza, nazionale o pubblica, il benessere economico del paese, la difesa dell'ordine e la prevenzione dei reati, la protezione della salute o della morale, nonché la protezione dei diritti e delle libertà altrui, nel quadro di una società democratica.

Più di recente, il diritto è stato sancito anche dalla Carta dei diritti fondamentali dell'Unione europea (2000), che ha provveduto però a distinguerlo opportunamente dall'ulteriore diritto alla protezione dei dati di carattere personale. Così, all'articolo 7, troviamo la consueta formula, per cui "ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni". All'articolo 8, invece, la tutela dei dati personali prevede che "tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica".

Tuttavia, uno dei paradossi cui va incontro il diritto alla privacy come diritto al rispetto della vita privata, riguarda la difficoltà di precisarne il significato; può infatti applicarsi alla privacy, ciò che abbiamo segnalato a proposito del fenomeno giuridico in generale e, cioè, l'impossibilità di esaurirne la ricchezza semantica, normativa e valoriale, nello spazio di un'unica formula (§ 1.1.2).

Per dare conto della tesi, è sufficiente riprendere cinque definizioni del concetto di privacy che, pur mettendo in chiaro questo o quell'aspetto della tutela del diritto, finiscono nondimeno per essere fuorvianti, se assolutizzate.

In primo luogo, possiamo declinare il concetto con le parole del giudice della Corte suprema nordamericana, William Brennan, nel caso *Eisenstadt vs. Baird* (1972), per cui la privacy consisterebbe "nel diritto dell'individuo di essere libero da intrusioni pubbliche [*government*] non autorizzate". Il punto debole della tesi che individua l'essenza della privacy nel diritto di non essere disturbati, e cioè come "non intrusione" da parte del governo, oppure dei privati, consiste nel fatto che simili approcci equiparano la privacy all'idea (negativa) di libertà. In questo modo, però, si rischia di perdere di vista che la privacy è ciò che rende possibile l'esercizio di una data libertà, non coincidendo, tuttavia, con la libertà stessa o con la condizione, o contenuto, con cui l'istituto è volta per volta associato.

In secondo luogo, ci si riferisce all'idea di privacy per evidenziare uno specifico diritto di escludere gli altri dalla propria vita, di vivere conseguentemente appartati, in santa pace e tranquillità. Rispetto alla prima definizione dell'essere "indisturbati", questa ha il vantaggio di proporre con la nozione dello "stato di solitudine" (v. Westin 1967), o d'"inaccessibilità" (v. Gavison 1980), un profilo eminentemente descrittivo dell'istituto, evitando sia la confusione tra privacy e libertà, sia tra il contenuto o la condizione della privacy e il rispettivo diritto. Nondimeno, anche l'idea della privacy come "esclusione" presta il fianco a una grave obiezione: com'è ben chiaro al lettore, ci sono in fondo molti casi in cui disponiamo di privacy e, però, non siamo affatto soli, godendo di privacy tra gli amici, o anche in pubblico.

In terzo luogo, alcuni autori hanno definito la privacy in termini di informazioni e, cioè, come "la zona" in cui l'accesso all'informazione personale è ristretto o limitato: di qui, in sostanza, che la "privacy perfetta" sia quella in cui nessuno ha informazioni su un soggetto determinato (v. Allen 1988: 269). Evitando di confondere la nozione di privacy con l'autonomia, la libertà o la solitudine degli individui, tuttavia, questa nuova accezione della privacy come "limitazione" ha il difetto di identificare a sua volta la privacy con la nozione di segretezza. Il risultato è di perdere di vista il ruolo che il controllo e le scelte personali svolgono nell'occasione, perché, appellandomi ancora una volta all'esperienza dei lettori, dovrebbe essere chiaro che solo chi ha privacy può scegliere di condividere con alcuni una certa informazione, nello stesso momento, o modo, in cui decide invece di escluderne altri.

In quarto luogo, secondo una prospettiva popolare negli Stati Uniti d'America, si ritiene che l'essenza della privacy vada trovata nel controllo che gli individui hanno sulle proprie informazioni, ponendo in questo caso l'accento sul ruolo che le scelte personali hanno nell'esercizio di questo diritto: la privacy "non è la semplice assenza di informazione su di noi da parte di altri, ma piuttosto è il controllo sull'informazione che abbiamo su noi stessi" (Fried 1990: 54). Rimanendo ancora poco chiaro il tipo d'informazione che uno ritiene debba rimanere sotto il proprio

controllo e il tipo di controllo che uno spera di poter esercitare, questo approccio alla privacy incorre però nell'errore eguale e contrario all'idea di privacy come "limitazione". Nel confondere privacy e autonomia, infatti, si giunge ad affermare, in coerenza con i propri assunti, che pure svelando volontariamente ogni singolo dato della propria vita a tutti – come spesso accade in certi spettacoli televisivi italiani – orbene, non per questo avremmo perso la nostra privacy.

In quinto luogo, si è cercato di porre rimedio ai limiti e paradossi delle precedenti teorie della privacy, proponendo una via di mezzo tra "accesso ristretto" e "controllo limitato" (Tavani 2007). Per un verso, è ammessa l'importanza della "situazione" in cui il singolo va protetto "dall'intrusione, interferenza o accesso alle informazioni da parte di altri" (Moor 1997: 30). D'altro canto, rispetto alla teoria della privacy come limitazione, è riconosciuto il ruolo del controllo e delle scelte personali, perché se è "possibile avere privacy senza avere controllo completo" sui propri dati personali, del pari si può "avere controllo sull'informazione senza avere privacy" (Tavani 2007: 11). Di qui che la privacy possa concepirsi come protezione rispetto a una situazione determinata, per la quale è dato però graduare il controllo mediante la scelta, il consenso o la revoca da parte dell'interessato. Nondimeno, anche integrando in questo modo le versioni della privacy come accesso ristretto e controllo limitato, rimane irrisolto un nodo fondamentale: non è dato stabilire, in effetti, se e per quali motivi la privacy sia un diritto autonomo o derivato da un insieme di ulteriori diritti; e cioè, se il suo valore sia intrinseco o puramente strumentale.

Potremmo allungare la lista con ulteriori definizioni di privacy; ma, riassunte le precedenti cinque con la prima figura del presente capitolo (v. figura 18 qui sotto), sorge naturale la domanda: come orientarsi innanzi a simile complessità?

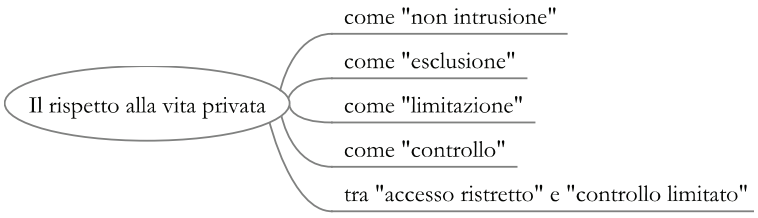


Figura 18: *La complessità della privacy*

Una via per procedere con l'analisi è di assumere per il momento una definizione "leggera" o minimale del concetto di privacy, che dia conto delle sue diverse accezioni in termini di non intrusione, esclusione, limitazione, controllo e accesso ristretto. A tal fine, soccorre la riflessione della filosofa tedesca Hannah Arendt (1906-1975), la cui tesi principale, non a caso, si trova come epigrafe del presente capitolo.

In sostanza, si tratta di cominciare a pensare alla privacy come ciò che rendendo visibile e profonda la nostra vita nel rapporto con gli altri, deve come tale rimanere opaco, invisibile o nascosto sullo sfondo, per non rendere la vita piatta. A partire da queste coppie di opposizioni elementari tra visibile e invisibile, trasparente e opaco, piatto e profondo, l'intento è di approfondire questi temi in rapporto ai tre punti principali sui quali ruota la riflessione dei prossimi paragrafi.

Innanzitutto (§ 6.1), l'attenzione verterà su come la tecnologia abbia contribuito a modificare profondamente il senso di quelle stesse opposizioni elementari: basti per ora dire che quando Arendt sviluppa le proprie riflessioni sulla privacy ne *La condizione umana* (1958), la filosofa pensa ancora alle quattro mura domestiche come presidio di ciò che, rimanendo opaco, rende profonda la vita. Oltre mezzo secolo dopo è chiaro come la rivoluzione delle tecnologie dell'informazione e comunicazione abbia del tutto spiazzato questo modo tradizionale di concepire la privacy. Per cogliere il significato di questo riposizionamento, il richiamo andrà alla fotografia (§ 6.1.1), alle banche dati (§ 6.1.2) e al Web 2.0 (§ 6.1.3).

Dopo di che (§ 6.2), il fuoco dell'indagine s'incentrerà sul modo in cui la tecnologia abbia profondamente mutato il rapporto tra sorvegliati e sorveglianti. Per secoli, lo scopo dei sorveglianti era ovviamente quello di controllare i sorvegliati, e di venire così a conoscenza dei loro segreti e pensieri; ora, si dà il caso di sorveglianti che sono anche in possesso di dati personali e intimi dei sorvegliati, di cui neanche questi ultimi sono a conoscenza! Questo scenario si è materializzato ai tempi della cosiddetta guerra al terrore (§ 6.2.1), nel più ampio contesto definito come società della nuova sorveglianza (§ 6.2.2). Ciò ha indotto molti a parlare di una presunta morte della privacy (§ 6.2.3); sebbene, all'atto pratico, occorra avvertire come esistano anche i dispositivi tecnologici a tutela dell'istituto (§ 6.2.4).

Per comprendere i riflessi giuridici delle trasformazioni in corso, l'ultima parte del capitolo si soffermerà sulla complessità sistemica del problema, ossia il fatto che il tema della tutela giuridica della privacy abbia più spesso natura internazionale o transnazionale, più che nazionale (§ 6.3). La fitta rete di disposizioni sia coercitive sia di diritto soffice, tra taxis e kosmos, sia sul piano transnazionale (§ 6.3.1), sia internazionale (§ 6.3.2), nulla toglie evidentemente alla circostanza che il piano nazionale di tutela continui a essere rilevante e, anzi, che esistano differenze sensibili tra gli ordinamenti giuridici nazionali (§ 6.3.3). A conferma, la parte conclusiva del capitolo servirà a introdurre l'analisi di quel particolare modello di tutela della privacy che è dato dal sistema giuridico nordamericano.

## 6.1. *Riposizionamenti tecnologici*

Per cominciare a cogliere il modo in cui la tecnologia incide sulle opposizioni tra ciò che è visibile e ciò che viceversa deve rimanere invisibile, dobbiamo risalire alla prima esauriente fondazione giuridica dell'istituto della privacy, vale a dire il saggio, diventato oramai un classico, che due giuristi nordamericani, Samuel Warren (1852-1910) e Louis Brandeis (1856-1941), pubblicarono sulla *Harvard Law Review* nel 1890: *The Right to Privacy* [1].

Sotto il termine di privacy, i due avvocati di Boston precisavano in sostanza il diritto che avrebbe dovuto godere di sì tanta fortuna nel XX secolo, e che presentavano ora come diritto di essere lasciati *alone* ossia "indisturbati" (Warren e Bran-

[1] Il numero delle pagine cui rimanda il testo, nel citare il saggio, è quello dell'edizione con testo originale a fronte, a cura del Garante per la protezione dei dati personali, Roma 2005.

deis 1890: 50); ora con la necessità di "ritirarsi dal mondo" e vivere isolati in casa propria (*op. cit.*, 53 e 117). L'obiettivo non era soltanto "di impedire che della propria vita privata si offra un ritratto non veritiero ma di impedire che questo ritratto sia in alcun modo eseguito" (*op. cit.*, 111).

Tuttavia, nel momento di spiegare i motivi delle garanzie da accordare al nuovo diritto, azionabile come tale davanti a un giudice nei confronti, soprattutto, dei privati cittadini, i due giuristi di common law andavano incontro a un non piccolo problema. Avendo presente la natura giurisprudenziale dell'ordinamento statunitense (§§ 3.2 e 4.1.2), imperniato sul principio dello *stare decisis*, Warren e Brandeis potevano vantare pur sempre pochi precedenti: oltre le citazioni del giudice Thomas C. Cooley, essi menzionavano il caso del Principe Alberto contro Strange, quello di Abernethy contro Hutchinson, e pochi altri (*op. cit.*, 67 e 83). Di qui, come creare legittimamente diritto senza ricorrere all'intervento del legislatore? Come difendere la tesi della necessità di tutelare un nuovo diritto, come quello alla privacy, all'interno di un sistema che s'ispira al principio dello *stare decisis*?

La risposta di Warren e Brandeis è semplice quanto brillante: non solo il diritto è qualcosa di vivo che evolve, nello stesso modo in cui evolvono il linguaggio e la specie umana, ma l'ordinamento deve anche prendere in considerazione le "nuove esigenze della società" che vanno di pari passo con il progresso tecnologico.

Ricostruendo, infatti, a grandi linee, la storia del common law negli Stati Uniti, la tesi è che, all'inizio, la legge "offriva rimedio soltanto contro l'ingerenza fisica nella vita e nei beni, contro gli atti violenti di trasgressione" (Warren e Brandeis 1890: 45). Soltanto in un momento successivo, sarebbe stata riconosciuta la natura spirituale, e non già solo fisica, dell'uomo, per cui alla protezione da immissioni o minacce fisiche vennero aggiunte le garanzie a tutela della reputazione nei confronti di affermazioni diffamatorie o non veritiere, e la protezione dei beni e diritti immateriali, come quelli che scaturiscono dai prodotti dell'intelletto. Questa "splendida abilità di crescere che caratterizza il common law [e che] permette ai giudici di approntare la protezione necessaria senza l'intervento del legislatore" (*op. cit.*, 51), era per ciò chiamata in causa per rispondere alle sfide poste dalle scoperte e le "recenti invenzioni" dell'uomo. L'esempio che i due avvocati di Boston davano, per mostrare tutta la potenza creatrice dell'homo technologicus (v. § 1.1), erano le prime fotografie istantanee che la Eastman Kodak Company veniva producendo fin dal 1884. Come diremo a continuazione, c'era la consapevolezza che le nuove macchine fotografiche avrebbero provocato casi inediti, a cui, appunto, il common law, nella "sua eterna giovinezza", avrebbe dovuto trovare rimedio.

### 6.1.1. *Fotografie*

Alla base del nuovo diritto alla privacy, Warren e Brandeis scorgono un nesso indissolubile tra progresso tecnologico, esigenze sociali e mutamenti "necessari" del diritto. La loro definizione della privacy come diritto a essere lasciati indisturbati è infatti legata a doppio filo alla nuova necessità di ritirarsi dal mondo che deriva dall'intensità e complessità della vita moderna. A ben vedere, l'invenzione delle macchine per fotografie istantanee andava a innestarsi nell'allora già fiorente mercato del giornalismo popolare d'impresa se, negli Stati Uniti del 1890, ai tempi di *The*

*Right to Privacy*, esistevano ben 900 quotidiani con più di 8 milioni di lettori. Pertanto, era ben chiaro a Warren e Brandeis che il mancato controllo della persona sulle proprie foto avrebbe sollevato questioni giuridiche nuove, dato che venivano trasformate alla radice le stesse modalità secondo cui è possibile eseguire tecnicamente un ritratto e, dunque, identificare un individuo. Dal quadro di un nobile, poniamo, ad opera di Anthony van Dyck (1599-1641), si era passati al dagherrotipo per il quale era richiesto ai nostri antenati qualche interminabile secondo per avere il proprio ritratto, fino al 1884, quando ha avuto inizio l'odierno popolare "cheese".

Come sarebbe diventato ovvio di lì a poco, con la battaglia a colpi di articoli sensazionalistici tra il *New York World* di Joseph Pulitzer (1847-1911), e il *New York Journal* di William Randolph Hearst (1863-1951), la circolazione abusiva d'immagini personali, per la prima volta sfruttabile quasi in tempo reale su scala industriale alla fine del XIX secolo, era destinata a produrre un insieme micidiale d'interessi economici e commerciali, tra la morbosità della gente e l'esigenza di una nuova riservatezza cui il common law doveva provvedere con adeguati mezzi di tutela. Con le parole dei due avvocati di Boston, "che l'individuo abbia piena protezione della sua persona e della sua proprietà è principio tanto antico quanto il common law; tuttavia, di tanto in tanto è stato ritenuto necessario ridefinire l'esatta natura ed estensione di tale protezione. Mutamenti politici, sociali ed economici portano con sé il riconoscimento di nuovi diritti, e il common law, nella sua eterna giovinezza, cresce, venendo incontro alle nuove esigenze della società" (Warren e Brandeis 1890: 51).

A differenza peraltro della vecchia Europa in cui, nei decenni a venire, la tutela della privacy sarebbe stata più spesso associata alla tutela delle persone agiate, dei "borghesi", questo non era il solo caso della democratica America. Se, ancora nel 1902, i giudici distrettuali di New York respingevano le richieste di una giovane che, senza il suo consenso, si era vista "litografata" su 25 mila volantini della *Franklin Mills Flour* con lo slogan "Flour of the Family", è significativo che lo stato di New York vi abbia posto rimedio soltanto un anno dopo (1903), con il § 51 del *N.Y. Civil Rights Act* tuttora in vigore. Due anni più tardi, era il turno della Corte della Georgia a riconoscere l'istituto tra i casi di responsabilità civile previsti dal common law: asserito che "il diritto alla privacy nelle materie puramente private è per ciò derivato dal diritto naturale", la corte provvedeva di conseguenza a tutelarlo nel caso *Pavesich vs. New England Life Insurance Co.* (50 S.E. 68 (Ga. 1905)).

Nell'evoluzione dell'ordinamento, era nato un nuovo diritto: *The Right to Privacy*.

### 6.1.2. *Banche dati*

Il secondo ricavato tecnologico sul quale vale la pena di attirare l'attenzione, riguarda la creazione di banche dati sempre più massicce e potenti, introdotte negli apparati burocratici e amministrativi del *welfare state* in paesi come la Svezia e la Germania tra gli anni cinquanta e sessanta del secolo scorso. L'opera sistematica di schedatura, monitoraggio e controllo sulle persone non ha dovuto attendere, naturalmente, tale perfezionamento della tecnologia; ma, proprio il ricordo delle schedature di massa nei regimi totalitari ha suggerito ai legislatori più accorti i nuovi problemi posti dalla sempre più efficiente raccolta ed elaborazione di dati personali in una società democratica. Alla tradizionale tutela della vita privata degli individui ri-

conosciuta, come detto, dalla Dichiarazione universale del 1948 e dalla Convenzione europea del 1950, è andata così facendosi strada l'idea di affiancare un'ulteriore tutela, ossia la protezione della privacy informativa delle persone come tutela dei loro dati personali. Da questo punto di vista è altamente significativo che la prima forma di tutela legislativa in Italia sia occorsa con la legge 300 del 20 maggio 1970, vale a dire con lo Statuto dei lavoratori, che regola la legittimità delle apparecchiature di controllo, anche a distanza, dei lavoratori (articolo 4), e vieta di fare indagini sulle loro opinioni (articolo 8).

All'originaria definizione della privacy come diritto di essere lasciati indisturbati, subentra in questo modo l'idea, recepita in molti ordinamenti europei tra gli anni settanta e ottanta del secolo scorso, che la partita si giochi sul fronte dei dati. Ne è conferma la prima legge svedese in materia del 1973 che, non a caso, è intitolata *Datalagen*, cui fa séguito nel 1977 la prima normativa federale dell'allora Germania dell'ovest che, a sua volta, si intitola *Bundesdatenschutzgesetz*. Quando, nel 1995 è stata introdotta nel diritto comunitario la prima disciplina sulla privacy con la direttiva 46, non è dunque a caso che la protezione sia stata accordata agli "individui riguardo alla elaborazione dei dati personali e al libero movimento dei suddetti dati" (come recita appunto il titolo della direttiva).

A scanso di possibili equivoci, tuttavia, occorre ribadire la tensione dialettica tra gli effetti regolativi della tecnica, il diritto e la società, su cui siamo venuti insistendo dalla introduzione di questo volume e, poi, nel capitolo primo (§ 1.2). Non si tratta infatti di suggerire un rapporto unidirezionale in base al quale la tecnologia è semplicemente la causa che detta i tempi dell'ordinamento giuridico, quasi che alle macchine fotografiche debbano seguire le leggi sulla privacy e alle banche dati quelle sulla protezione dei dati. A conferma, basterà far caso ad altri e ulteriori parametri, per i quali, ad esempio, è indicativo che negli Stati Uniti d'America manchi un'analoga disciplina generale in materia di trattamento e tutela dei dati personali a livello federale. La circostanza si spiega, ora, con il diverso peso e ruolo assegnato alle forze economiche del mercato e con l'idea della loro auto-regolamentazione; ora, per via del fatto che gli Stati Uniti, a differenza dell'Europa, non hanno conosciuto in casa propria i fenomeni del totalitarismo nazi-fascista e comunista. Ciò non significa che non esistano leggi federali statunitensi in materia; ma, appunto, per via della diversa tradizione, cultura e storia di quel paese, l'approccio è stato diverso, ossia settoriale e pragmatico, volta per volta teso a colmare i vuoti normativi prodotti dal progresso e l'evoluzione tecnologica. Anticipando temi e motivi dei prossimi paragrafi, abbiamo così, da un lato, il *Cable Communications Policy Act* del 1984, l'*Electronic Communications Privacy Act* del 1986, l'*Identity Theft and Assumption Deterrence Act* del 1998, e il *Video Voyeurism Prevention Act* del 2004, cui vanno aggiunte due leggi con le quali abbiamo già qualche dimestichezza, ossia il *Health Insurance Portability and Accountability Act* o HIPPA del 1996 (si v. § 5.3.2), e il *CAN-SPAM Act* del 2003 (su cui invece si v. § 1.4.3).

D'altro canto, un'altra specificità del modello statunitense riguarda il fatto che, spesso, l'intervento del legislatore federale ha di mira i poteri del governo, più che la disciplina del rapporto tra i privati in materia di privacy e protezione dei dati personali. Al posto dei vuoti normativi creati dall'evoluzione tecnologica, il riferimento va agli scandali occorsi, più spesso, a partire dagli anni settanta del '900, cui il congres-

so di Washington ha inteso volta per volta porre rimedio. Questo spiega perché, come riferiremo (§ 6.2.1), il legislatore statunitense non si sia ancora occupato a fondo del tema di questo paragrafo – e cioè, appunto, le banche dati – ma abbia preso di mira piuttosto le intercettazioni ambientali dei politici o i gusti cinematografici dei giudici. Basti pensare al *Privacy Act* del 1974 che fece séguito allo scandalo del Watergate con le dimissioni del presidente Richard Nixon (1913-1994); oppure, il *Video Privacy Protection Act* del 1988, approvato dal Congresso poco dopo quello che era capitato al giudice Robert Bork, del quale, durante le audizioni per la conferma a membro della Corte suprema, la stampa finì per pubblicare la lista delle videocassette prese a noleggio; e che, per sua fortuna, comprendeva soltanto titoli come *Un giorno alle corse* dei fratelli Marx o *Ruthless people* con Bette Miller e Danny DeVito.

Il fatto, poi, che dal 1988 a oggi, la gente abbia smesso di andare da Blockbuster, poniamo, per noleggiare una videocassetta, ma visiti Netflix, Redbox o Video Ezy, per non parlare di altri canali del fiorente circuito in streaming o con le reti P2P, sta a indicare le ulteriori sollecitazioni della tecnologia con le nuove questioni di privacy e di protezione dei dati che si trascina dietro. Tra i tanti esempi possibili, concentriamoci a continuazione su quello del Web 2.0.

### 6.1.3. *Web 2.0*

Tra le reti della rete d'internet, una delle più note al grande pubblico è senz'altro quella del world wide web (www), inventata da un informatico britannico che abbiamo già avuto modo di ricordare nel capitolo terzo (v. § 3.4.2). Al lavoro presso il CERN di Ginevra, nel 1989, l'idea di Berners-Lee è stata di connettere la tecnologia degli ipertesti all'architettura d'internet, in particolare al protocollo per il controllo della trasmissione delle informazioni in rete (TCP), e al sistema dei nomi a dominio (DNS), tramite un nuovo protocollo, quello appunto del trasferimento ipertestuale (http), tra un "client" e un "server". Il Web è perciò un sistema informativo, distribuito e ipermediale, ossia una rete di risorse informazionali che sfrutta e potenzia l'apertura dell'architettura d'internet, il suo principio "end-to-end", su cui si è attirata l'attenzione nel capitolo quinto (§ 5.4.1). Per dirla con le parole del suo inventore, l'architettura del Web è stata cioè disegnata in modo tale da essere anch'essa "fuori controllo" (Berners-Lee 1999).

Un ulteriore passo in questa direzione si è poi avuto all'inizio del secolo XXI, quando si è cominciato a parlare di un Web 2.0, per mettere in risalto il nuovo ruolo degli utenti nella rete: se, in ciò che in retrospettiva possiamo definire il Web 1.0, l'utente appariva come un passivo ricettore di dati e informazioni, viceversa, nel Web 2.0, si è cominciato ad assistere a un'inedita interattività, per la quale i contenuti sono più spesso prodotti dagli utenti della rete, con la possibilità di immettere e condividere direttamente le informazioni nel sistema, dove altri utenti potranno selezionare e rivedere a loro volta i dati. Si tratta del passaggio che, tra le altre cose, ha condotto dall'enciclopedia Britannica online (Web 1.0) a Wikipedia (Web 2.0), dalle prime pagine personali web ai blog, dagli elenchi tassonomici all'etichettature come il tagging, e via dicendo. Di qui che quando, nell'ultimo numero del dicembre 2006, la rivista "Time", come tradizione, ha eletto la persona dell'anno, il premio sia

stato assegnato a ciascuno di noi: "You". Con le motivazioni del premio: "Yes, you. You control the Information Age. Welcome to your world".

Rispetto all'ottimistico quadro d'assieme offerto dalla rivista americana, il successo del Web 2.0 ha però comportato una serie di nuovi problemi giuridici che, in parte, derivano dalla circostanza che gli utenti non controllano affatto i loro dati nell'età dell'informazione. Da un lato, è il caso dei rischi connessi alla possibilità di caricare nella rete, senza alcuna mediazione o filtri di sorta, dati e informazioni su terzi, oppure del costume invalso in molti social network di creare pagine e profili di soggetti che abbiamo incontrato o che avremmo voluto conoscere, attribuendo loro un punteggio, immagini o quant'altro, senza che il diretto interessato ne sia minimamente a conoscenza. D'altro canto, è la stessa architettura del web e d'internet a esporre gli utenti agli ulteriori rischi connessi alla diffusione di virus informatici, spam e phishing, con furti d'identità digitali e altro ancora. Il risultato è che, al pari delle precedenti innovazioni tecnologiche, come nel caso delle macchine fotografiche o le banche dati, anche il web ha contribuito a modificare profondamente il modo di concepire la tutela della vita privata.

Per quasi un secolo, l'idea del rapporto tra ciò che è visibile e ciò che deve invece essere sottratto alla curiosità altrui, è stata infatti associata alla tutela della privacy come presidio del "proprio castello" o delle quattro mura domestiche, secondo un'immagine che abbiamo già segnalato con l'opera di Arendt. Questa è del resto l'immagine con cui retoricamente anche Warren e Brandeis concludevano *The Right to Privacy*: "Il common law ha sempre considerato la casa di un uomo come un castello, spesso inespugnabile per i suoi ministri incaricati di eseguirne le disposizioni. Vogliono forse i giudici chiudere la porta d'ingresso all'autorità costituita, e spalancare l'entrata di servizio ad un'oziosa o pruriginosa curiosità?" (*op. cit.*, 117). Questa è ancora l'immagine che, nel 1970, nel caso *Rowan vs. Post Office Department*, la Corte suprema nordamericana impiega per illustrare la propria decisione su un aspetto particolare della tutela della privacy in quel paese e, cioè, il diritto di non sentire le opinioni altrui: se "rendere il padrone di casa il giudice ultimo ed esclusivo di ciò che può attraversare la porta ha indubbiamente l'effetto di impedire la libera circolazione delle idee", tuttavia, "nulla nella Costituzione ci costringe a sentire o ricevere comunicazioni indesiderate, qualunque ne sia il contenuto" poiché, riprendendo appunto la conclusione di *The Right to Privacy* di Warren e Brandeis, "l'antico concetto che «la casa dell'uomo è il suo castello» non ha perso in alcun modo la sua vitalità" (397 U.S. 736-737).

Or bene, uno degli effetti più dirompenti della connessione universale dei computer con la loro interattività ha a che fare proprio con la vecchia idea di essere sicuri e garantiti in casa propria, chiudendone la porta dietro di sé. Si tratta di un processo eguale e contrario a quanto visto più sopra con l'uso della tecnologia delle telecamere di sorveglianza a circuito chiuso (CCTV), negli ambienti in cui viviamo e interagiamo (v. § 5.1.2). Se, in quella occasione, l'accento è stato posto sul modo in cui muti l'aspettativa di riservatezza delle persone negli spazi pubblici, qui, viceversa, occorre notare come tale aspettativa sia del pari cambiata dentro al "proprio castello" tra la fine degli anni novanta e l'inizio del nuovo secolo, tra il Web 1.0 e il 2.0, tramite l'interazione resa possibile dai computer in casa propria. L'invisibilità tradizionalmente garantita in senso fisico dalle pareti di un'abitazione, non soltanto

è stata spiazzata dalla crescente digitalizzazione della vita; ma, la nuova visibilità delle azioni domestiche, a contatto con le nuove tecnologie, non è che l'altra faccia della medaglia del processo di raccolta, trattamento e uso delle informazioni, anche sensibili sulle persone, diventato a sua volta invisibile.

Come vedremo a continuazione, la privacy degli individui, declinabile sempre più spesso come privacy informazionale nel nuovo contesto tecnologico, è messa a repentaglio dal processo di raccolta e trattamento dei dati che può dirsi appunto invisibile, perché immanente alle azioni quotidiane e attuato in forma continuativa, discreta e disponibile, al limite, in tempo reale. Dal riposizionamento della privacy con il web dei primi anni 2000 passiamo di qui al nuovo "castello" che le persone hanno in tasca con i propri telefonini.

## 6.2. *Riposizionamenti assicurativi*

La formula di questo paragrafo sui "riposizionamenti assicurativi" va interpretata alla lettera; ossia, come ciò che tende ad assicurare e, cioè, a garantire sicurezza.

Ci siamo già soffermati sul tema nel capitolo precedente, sia a proposito delle misure di sicurezza nel duplice senso di *safety* e *security* (§ 5.2.2), sia della finalità che il design può avere, ovvero di prevenire la possibilità che eventi dannosi si verifichino (§ 5.2.3).

Inoltre, tanto nell'introdurre il presente capitolo, quanto in rapporto alla legittimità del design a controllo totale (§ 5.4.3), si è fatto cenno al dato che la nozione di sicurezza, declinata nel senso della sicurezza nazionale o pubblica, costituisca un limite alla tutela e protezione della vita privata.

A questo punto, occorre completare il quadro, muovendo da quello che è stato un vero e proprio spartiacque della più recente storia contemporanea, vale a dire gli attacchi dell'11 settembre 2001 da parte di al Qaeda che portarono, tra le altre cose, al crollo delle Torri Gemelle a New York. La ragione è triplice.

Innanzitutto, la cosiddetta guerra al terrore dichiarata dal presidente statunitense George W. Bush all'indomani degli attacchi dell'11 settembre, ha prodotto una mole di provvedimenti normativi, senza i quali sarebbe difficile – per non dire impossibile – inquadrare oggi il regime della privacy.

Questi provvedimenti draconiani, in secondo luogo, hanno rimesso finanche in discussione alcuni capisaldi della tradizione costituzionale dei moderni (§ 3.1.3), al punto da riportare, più che al contrattualismo di Locke o di Rousseau, all'alternativa del contratto sociale di Hobbes in tema di sicurezza (§ 2.1.2.1).

Infine, affrontare i temi della privacy ai tempi della guerra al terrore, costringe ad approfondire i modi in cui la tecnologia ha svolto la sua parte. A quanto detto finora a proposito di CCTV, computer e banche dati, bisogna aggiungere altre modalità di controllo e sorveglianza, come i dispositivi di geo-localizzazione (GPS), la profilazione degli individui, le intercettazioni delle comunicazioni e altro ancora.

Molti di questi dispositivi, applicazioni e sistemi, sono naturalmente alla portata del settore privato, ciò che ha indotto tanti a parlare, in termini più generali, di una nuova società della sorveglianza, di cui quella ai fini della sicurezza nazionale e dell'ordine pubblico non sarebbe che un caso, sia pure tra i più preoccupanti e significativi.

Su queste basi si è giunti a un bivio che anima tuttora il dibattito: c'è chi dall'uso della tecnologia nel caso dei programmi per i fini della sicurezza nazionale e, in genere, con l'insieme di "osservabili" riassumibili nei termini della società della "nuova sorveglianza", ne ha ricavato, né più né meno, "la morte della privacy". Altri, invece, notano come i vari significati del termine "privacy" stanno cambiando, analogamente a come la nozione sia già mutata dai tempi del diritto a essere lasciati indisturbati di Warren e Brandeis (§ 6.1.1). Si tratta del percorso che, dall'originaria definizione dell'istituto, ha condotto alle forme di una privacy informativa con la nuova generazione di leggi in tema di protezione dei dati personali (§ 6.1.2), fino all'esplodere della rivoluzione informatica: la "quarta rivoluzione" (§ 1.4). Se, in quella sede, sono stati illustrati quattro osservabili dell'analisi con la figura 4, qui, bisogna invece specificare come i processi cognitivi del diritto (§ 1.4.1), i suoi istituti (§ 1.4.2), le tecniche (§ 1.4.3), e le istituzioni nell'era delle società ICT-dipendenti (§ 1.4.4), si riposizionino nei termini del rapporto tra il diritto alla privacy e, per dir così, il suo "opposto aristotelico", vale a dire ai sensi dell'articolo 8 della CEDU, il fine della sicurezza nazionale.

I due nuovi osservabili e le variabili dell'analisi sono illustrati con una nuova figura che il lettore troverà più sotto (figura 19). A partire da questo livello d'astrazione, l'indagine del presente paragrafo sarà scandita nel modo seguente: innanzitutto, esamineremo le due variabili del primo osservabile, ossia, i motivi della sicurezza e la privacy ai tempi della "guerra al terrore" (§ 6.2.1), nonché i temi della "nuova sorveglianza" (§ 6.2.2), che hanno indotto molti studiosi a concludere che la privacy sia morta (§ 6.2.3). Dopo di che, l'opposta serie di variabili, attinenti alla tutela della privacy nelle società ICT-dipendenti, verrà introdotta in un nuovo paragrafo (§ 6.2.4).

Rispetto ai quattro osservabili della "quarta rivoluzione", il lettore noterà che, assunti come variabili del nuovo modello della figura 19, essi sono passati da quattro a tre: la ragione dipende dal fatto che degli istituti della quarta rivoluzione (§ 1.4.2), uno, quello della privacy, viene qui assunto come punto di riferimento per indagare come mutino ora i processi cognitivi del diritto, ora le sue tecniche e istituzioni, ai fini della sicurezza, pubblica e privata.

Infine, di queste tre ultime variabili dell'indagine, si metterà specialmente in risalto l'ultima istituzionale, distinguendo ulteriormente tra il piano transnazionale, internazionale e nazionale, di tutela: è ciò che sarà analizzato a parte, all'insegna della "globalizzazione giuridica" (§ 6.3).

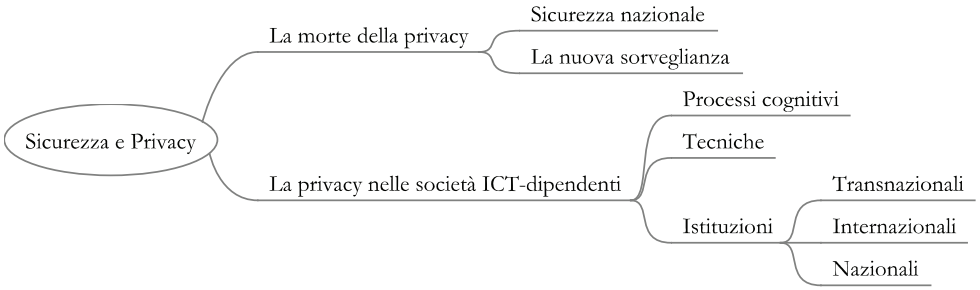


Figura 19: *La complessa tutela della vita privata oggi*

Proseguiamo quindi la nostra analisi sulla tutela della vita privata oggi, in rapporto al difficile rapporto tra sicurezza nazionale e privacy.

### 6.2.1. *La privacy ai tempi della "guerra al terrore"*

Uno dei settori più tormentati della privacy da oltre una decade, ha a che fare con la cosiddetta "guerra al terrore" dichiarata dall'allora presidente nordamericano George W. Bush, all'indomani del crollo delle Torri Gemelle. Il mese successivo agli attacchi dell'11 settembre, prima il Senato (11 ottobre 2001), e poi il Congresso (il 12 ottobre), approvarono l'*Atto anti-terrorismo*, cui ha fatto séguito, subito dopo, l'entrata in vigore del più ambizioso *USA Patriot Act* votato quasi all'unanimità dal Congresso il 23 ottobre e, il giorno dopo, dal Senato (Bush ha ufficialmente sottoscritto la legge il 26 ottobre 2001). Tenuto conto degli attacchi, il successivo 19 novembre venne poi approvato l'*Aviation and Transportation Security Act*, integrato successivamente da vari regolamenti del *Department of Homeland Security* (DHS), tra cui il *Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States*, pubblicato sul *Federal Register* il 31 dicembre 2001, e il *Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States*, pubblicato sempre sul *Federal Register* il 25 giugno 2002.

Secondo le riforme introdotte dal *Patriot Act*, è stata anche riorganizzata la fitta rete di agenzie federali preposte alla sicurezza interna del paese: il primo marzo 2003 il Dipartimento per la sicurezza nazionale (DHS) assorbiva le funzioni dell'*Immigration and Naturalization Service*, avvalendosi di un'apposita agenzia, la *Transportation Security Agency*, a sua volta istituita il 19 novembre 2001, stante il programma per la protezione della rete del trasporto aereo varato con la "guerra al terrore".

Oltre alle disposizioni in materia di sicurezza per il traffico aereo, il *Patriot Act* ha anche esteso i poteri investigativi dei giudici sul piano federale (§ 216A della legge). Fino alla riforma, gli ordini dei giudici di setacciare tabulati elettronici e segnali digitali erano validi solo per la sfera di competenza della giurisdizione di quel determinato giudice: di New York, di Los Angeles, ecc. Il *Patriot Act* ha così stabilito che gli ordini di un giudice coprano l'intero territorio nazionale, nell'utilizzo di sistemi di filtraggio e intercettazione delle informazioni, come, a quei tempi, con il programma *Carnivore* messo a punto dall'FBI. A seconda del settaggio, il filtro del sistema consentiva di tararlo in modo da visionare tutto il contenuto della comunicazione ("versione full"), o di limitarsi a rintracciare soltanto gli indirizzi elettronici ("versione light"). Questo è importante perché, nel 1986, con l'*Electronic Communications Privacy Act*, il Congresso aveva approvato una legge con cui si autorizzava non solo l'intercettazione della posta elettronica, registrando i numeri (IP, di telefono, o altro), così attivati; ma, tutto il contenuto dell'email e, anzi, di tutti i media utilizzati da una persona determinata (nel qual caso è però richiesta l'autorizzazione dell'*Attorney General*).

Inoltre, il *Patriot Act* ha provveduto a integrare ed estendere, e solo in parte a modificare, le norme del *Foreign Intelligence Surveillance Act* (FISA) del 1978, in modo tale che molte delle disposizioni che prima valevano soltanto nei confronti

degli stranieri, sono state estese ai cittadini americani: sebbene queste disposizioni si applichino solo per gli affari esteri del paese, questa distinzione di competenze tra affari interni ed esterni tende a sbiadire per via dello stesso progresso tecnologico. La legittimità del controllo, "full" o "light", di tutte le comunicazioni elettroniche di un numero crescente di persone si fonda infatti sulla repressione di ogni forma di terrorismo che, tuttavia, con la sezione 802 del *Patriot Act*, è stata di molto ampliata, punendo "gli atti pericolosi per la vita umana che rappresentano una violazione delle leggi penali degli USA o di ogni Stato [dell'Unione]" volti, ora, "all'intimidazione o costrizione della popolazione civile", ora, "all'influenza delle politiche di un governo con l'intimidazione o costrizione". Se, poi, si pensa che il *Patriot Act* richiede un semplice "motivo significativo" per cominciare a investigare su un soggetto sospetto, il risultato è che i cittadini americani si sono ritrovati in uno stato di sorveglianza, fitto e capillare, quanto quello sviluppato per i restanti cittadini del mondo. Nell'era delle società ICT-dipendenti, virtualmente ogni informazione può essere prima o poi rilevante ai fini della lotta al terrorismo, se è vero che anche i terroristi usano carte di credito, scrivono email, trasferiscono denaro via internet, visitano siti web, prenotano stanze d'albergo, e via di questo passo. Come diremo, il perno giuridico di questo sistema d'intercettazioni si fonda sulla sezione 512 del *Patriot Act*, sul quale mi sono soffermato a suo tempo (Pagallo 2008: 24-25); e il cui senso, tuttavia, le rivelazioni di Snowden nel 2013 hanno reso molto più esplicito.

A completare il quadro, sul piano processuale, è stata introdotta con la sezione 213 della legge una notevole restrizione anche sul piano delle garanzie: a differenza dei casi ordinari, in cui l'evidenza probatoria deve essere notificata al sospettato non appena raccolta, il *Patriot Act* consente di ritardare la comunicazione delle ricerche a carico dell'indagato per motivi di sicurezza, per ciò stesso a conoscenza delle prove solo nel corso dell'eventuale processo.

Su queste basi giuridiche, da un lato, l'agenzia di polizia federale sotto il dipartimento di giustizia, l'FBI, è venuta accumulando una mole impressionante di dati e informazioni sui propri cittadini, ora autorizzati da una corte ai sensi del § 512 del *Patriot Act*, ora in ragione delle "lettere di sicurezza nazionale" con cui l'agenzia federale richiede informazioni a terzi con una semplice richiesta scritta e, cioè, senza bisogno di alcuna autorizzazione giudiziaria nei casi riguardanti tale sicurezza nazionale. D'altro canto, sin dall'inizio dello scorso decennio, il ricordato Dipartimento per la sicurezza nazionale (DHS) è venuto approntando tutta una serie di programmi al fine di garantire la protezione del territorio, controllando il flusso delle informazioni in, per o dagli Stati Uniti, con gigantesche banche dati. Del progetto Matrix, abbandonato nell'aprile 2005, mi sono occupato a tempo debito (Pagallo 2008: 102-103); così come del programma per la sicurezza dei voli messo a punto dall'Agenzia per la sicurezza dei trasporti, sotto l'egida del DHS (*op. cit.*, 103-105). In quel libro, proseguivo l'analisi con un paragrafo dal titolo, purtroppo, profetico: nel ricordo di Ernst Hemingway (1899-1961), "per chi suona la campana?".

Essa è risuonata forte nel 2013 con lo scandalo sul progetto Prisma dell'Agenzia nordamericana per la sicurezza nazionale (NSA) e i cosiddetti file GCHQ britannici (v. § 5.4.2).

Dal punto di vista degli americani, lo scandalo non è consistito tanto nel fatto che l'NSA possa ascoltare le telefonate dei cittadini non americani, o leggere le loro

email, sulla base del sospetto che, in fondo, sono cittadini stranieri che vivono all'estero: per questo, c'è un'apposita legge del 2008, che autorizza l'NSA, stante un apposito emendamento al FISA, a condurre simili indagini.

Piuttosto, lo scandalo è consistito nel fatto che la sezione 512 del *Patriot Act* sia stata utilizzata per autorizzare l'NSA a implementare il suo programma di raccolta e trattamento dei "metadati" delle telefonate e comunicazioni elettroniche, quali luogo, ora, durata e destinatario della chiamata, anche nei confronti dei cittadini americani. Con le rivelazioni di Snowden, poi confermate da due documenti indipendenti di un gruppo di esperti istituito da Obama nel dicembre 2013, e del *Privacy and Civil Liberties Oversight Board*, nel gennaio 2014, si è saputo che l'NSA ha ammassato informazioni sui dati di geo-localizzazione, dati personali sui telefoni cellulari, indirizzari di posta elettronica, oltre a intercettare il flusso di dati transfrontalieri dei server di giganti del settore, come Google e Yahoo. A giudizio del *Privacy Board*, l'agenzia federale indipendente a tutela della privacy e delle libertà civili, istituita dal Congresso nel 2004, si calcola che in questo modo i (meta)dati telefonici di 120 milioni di cittadini americani siano sotto controllo ogni anno.

A peggiorare le cose sul piano giuridico, la sezione 512 del *Patriot Act* non fa riferimento in nessun modo all'NSA, bensì all'FBI, per chiedere l'autorizzazione a raccogliere dati che si ritengono rilevanti per condurre attività di sicurezza e antiterrorismo. Inoltre, l'organo della iurisdictio preposto al controllo dell'NSA, cioè la *Foreign Intelligence Surveillance Court* (FISC), ne ha rinnovato periodicamente, ogni 90 giorni, l'autorizzazione per condurre il programma per la raccolta dei metadati in modo routinario. Del resto, la Corte agisce in segreto, sente solo gli avvocati dell'esecutivo, accogliendone quasi sempre le richieste, e non rendendo pubblici i suoi ordini.

Come riferito nel capitolo precedente (§ 5.4.3), un giudice distrettuale della Columbia, nel dicembre 2013, ha dichiarato illegittime due disposizioni chiave del programma dell'NSA nel caso *Klayman vs. Obama*. Il presidente americano, nondimeno, ha sostanzialmente difeso il programma il 17 gennaio 2014, concedendo però che l'NSA possa avere accesso ai dati soltanto con l'autorizzazione del giudice e per una ricerca specifica; e che, in ogni caso, d'ora in avanti i dati dovranno essere custoditi da terzi (sebbene tutte le grandi imprese del settore, come IBM o Google, abbiano dichiarato da subito di non essere affatto interessate a tale custodia).

Dal punto di vista del diritto costituzionale, la questione ruota sull'interpretazione da dare al quarto emendamento alla costituzione nordamericana e alla giurisprudenza della Corte suprema: in particolare, il richiamo va al caso *Smith vs. Maryland* del 1979, in cui la Corte di Washington ha ritenuto legittimo l'uso da parte della polizia di sistemi per la rintracciabilità e registrazione dei numeri composti dal sospetto ("pen register"), senza alcuna autorizzazione del giudice. In quella occasione, la Corte ha formulato la "regola della divulgazione a terzi", per cui chiunque condivida le proprie informazioni volontariamente con altre persone o enti, rinuncerebbe per ciò stesso a una ragionevole aspettativa di privacy. Il ragionamento seguìto, al fine di giustificare queste operazioni di polizia senza mandato, è che siccome ciascuno di noi condivide con la propria compagnia telefonica i numeri composti quando fa una chiamata, non ci sarebbe dunque spazio per una ragionevole aspettativa di vedere tutelata in questo caso la propria privacy.

Sul punto torneremo nel prossimo capitolo, quando esamineremo in dettaglio il quarto emendamento alla costituzione americana. Per ora, basti dire che in molti si sono spinti fino al punto di constatare, o denunciare per questa via, la fine della privacy. Come diremo a continuazione, l'idea è in fondo quella che la nostra sia la società della nuova sorveglianza.

### 6.2.2. *La società della "nuova sorveglianza"*

L'assunto di base della "nuova sorveglianza" non si limita a sottolineare l'aggiornamento tecnologico del modo in cui si esplicita appunto l'attività del sorvegliare, vale a dire, per riprendere un noto dizionario italiano, l'"osservare, seguire con attenzione qualcuno o qualcosa per prevenire o reprimere eventi non voluti, dannosi, illeciti o controllare il regolare svolgimento di un'attività, garantire la normalità di una situazione, seguire l'evoluzione di un procedimento o simili". In realtà, con la formula della "nuova sorveglianza" si vuole mettere in evidenza come il significato di questo "osservare" o di "seguire con attenzione qualcuno o qualcosa" sia cambiato profondamente con le inedite modalità di controllo per la sicurezza messe a disposizione dalla tecnologia; come, ad esempio, quando si afferma che i genitori sorvegliano i propri figli tramite il GPS dei loro cellulari, o il governo bada alla sicurezza dei propri confini, pattugliandoli a mezzo di robot.

Il nuovo significato che finisce per acquisire, in questa prospettiva, la nozione del sorvegliare, comporta tuttavia la necessità di distinguere accuratamente due piani del discorso, ossia il piano descrittivo di come muti, o sia già cambiato, il significato del sorvegliare e la valutazione che intendiamo dare dei processi in corso. Per approfondire questo duplice piano, vale la pena d'incentrare l'attenzione in questa sede su tre protagonisti della nuova sorveglianza: lo stato, le imprese private nel settore delle telecomunicazioni e dei servizi, e "You" (§ 6.1.3). Proprio come la persona 2006 di Time magazine: "Yes, you. You control the Information Age. Welcome to your world".

La ragione iniziale per cui si ha di mira il gubernaculum e, più in particolar modo, l'esecutivo degli stati nazionali come primo protagonista della nuova sorveglianza dipende dai compiti di controllo, volti a garantire la sicurezza e l'ordine pubblico, che sono stati il tradizionale appannaggio esclusivo degli stati nel corso dei secoli. Quando si è avuta la Dichiarazione universale del 1948 (v. § 5.4.3), non è dunque a caso che un'apposita disposizione abbia disciplinato questa essenziale funzione del gubernaculum, tenuto a rispettare, sia pure entro certi limiti, la vita privata degli individui. È, però, questo bilanciamento tra privacy e sicurezza, come abbiamo cominciato a segnalare nel paragrafo precedente, a esser stato posto a repentaglio, a partire dallo spartiacque degli attacchi dell'11 settembre. Alla fitta rete di norme, regolamenti e sistemi operativi di sicurezza, introdotta negli Stati Uniti, bisogna ora aggiungere i provvedimenti presi anche al di qua dell'Atlantico. Nel dicembre 2001, il Parlamento di Westminster approvava l'*Anti-terrorism, Crime and Security Act*, introducendo una serie di misure draconiane sui controlli, fermi di polizia e garanzie giurisdizionali dei sospettati; dopo di che, il 12 luglio 2002, il Parlamento europeo e il Consiglio hanno approvato la nuova direttiva su privacy e telecomunicazioni, che ha modificato profondamente la precedente direttiva D-1997/66/CE. Con le

norme di D-2002/58/CE è previsto che la legislazione degli stati membri possa obbligare i provider di internet (ISP) e le società di telecomunicazioni a trattenere e conservare i dati dei propri utenti per lunghi periodi di tempo. Ad esempio: l'Italia ha provveduto a recepire la normativa, emendando una prima volta il decreto legislativo 196 del 30 giugno 2003 – il cosiddetto "codice della privacy" italiano – con il decreto legge 354 del 24 dicembre 2003, convertito in legge dal Parlamento il 26 febbraio 2004 (legge 45). Ai sensi dei successivi interventi del legislatore, il tormentatissimo articolo 132 del codice sulla "conservazione dei dati di traffico per altre finalità" stabilisce che i dati relativi alle telefonate degli utenti siano conservati per almeno due anni, rispetto agli iniziali quattro; salvo poi prevedere, nei casi d'investigazioni ai sensi dell'articolo 132.4 *ter*, l'estensione del periodo di conservazione dei dati per altri sei mesi.

La tradizionale sorveglianza condotta in questo modo dagli stati risulta tuttavia "nuova", stante il salto di qualità provocato dall'uso delle più recenti tecnologie. Oltre al repertorio di sistemi per la conservazione dei dati o il filtraggio onnipervasivo della rete, come proposto dalla Commissione europea nel 2010 (v. § 5.2.3), e i programmi delle agenzie di sicurezza americane su intercettazioni, banche dati e raccolta di metadati (§ 6.2.1), è il caso di aggiungere alle tecniche del GPS, alla biometria, al DNA o alle vecchie impronte digitali, le nuove frontiere dischiuse dalle applicazioni robotiche. Mentre una buona metà delle ricerche nell'ambito dell'intelligenza artificiale (§ 1.4.1), vengono sponsorizzate dalle forze armate americane, le ricadute civili di queste ricerche sono diventate del tutto evidenti dall'inizio di questa decade, come attesta l'esempio dei droni, impiegati sempre più spesso dalle forze dell'ordine ai fini della sorveglianza, sicurezza e controllo. Avendo a mente come molti scenari di fantascienza si siano nel frattempo materializzati (§ 1.4.4), di qui a giungere all'uso di una nuova generazione di "RoboCop", secondo la saga hollywoodiana (1987 e 2014), il passo sembra breve.

Il secondo protagonista della "nuova sorveglianza" è certamente il settore delle compagnie private, soprattutto nell'ambito delle telecomunicazioni e dei servizi in rete. In fondo, tutti noi cediamo volontariamente, su basi quotidiane, i nostri dati per acquistare libri, visitare siti, aggiornare la pagina personale sulle piattaforme sociali, nei blog, con l'uso delle carte di credito, nelle prenotazioni, e via dicendo, per cui Amazon "sa" dei miei gusti in fatto di libri, musica e video; Google del contenuto delle mie email e le mie interrogazioni in rete; eBay dei miei acquisti; Facebook della mia rete sociale; WhatsApp e Twitter dei miei messaggi quotidiani; ecc. Buona parte di questa interazione è gestita dai fornitori di servizi, sfruttando i progressi della intelligenza artificiale, come nel caso del *machine learning*, ossia dei programmi per l'apprendimento delle macchine o dei sistemi informatici che aumentano la qualità dei servizi e prestazioni, grazie alla "propria esperienza". L'automazione dei servizi ha fin qui offerto un equilibrio tra le aspettative di riservatezza da parte degli utenti, e le esigenze commerciali delle imprese, secondo un modello di auto-regolamentazione e concorrenza tra i diversi fornitori di servizi nelle società ICT-dipendenti, che abbiamo visto essere una delle caratteristiche del modello nordamericano della privacy (§ 6.1.2). Inoltre (§§ 4.3.3.2-3), il rapporto tra utenti e gestori si fonda spesso su un rapporto di fiducia che, tuttavia, può portare a quelle forme di protesta, talora molto efficaci, come occorso ai primi tempi di Facebook (§ 5.1.3).

A ben vedere, sono due i motivi principali per cui questo meccanismo d'autoregolamentazione, concorrenza e fiducia tra privati, può incrinarsi.

Da una parte, la raccolta e lo sfruttamento dei dati, nell'era delle società ICT-dipendenti, sono diventati il cuore del modello di business per molti giganti dell'economia. Mentre, a metà degli anni 2000, destava ancora stupore il miracolo di un sistema, come quello della rete, fondato sull'offerta, all'apparenza gratuita, di una molteplicità di servizi – come, ad esempio, nella galassia Google, o più tardi in Facebookistan – nondimeno, di lì a poco, sarebbe diventato del tutto evidente come una delle fonti principali, dalla quale quelle stesse imprese traevano le proprie fortune, fosse la "compravendita" dei dati personali. Sul piano giuridico, i rapporti tra gli utenti e il fornitore di servizi dipendono, per buona parte, dai termini dello stesso servizio che viene offerto dall'impresa. Anche ad ammettere i limiti posti dalle legislazioni a tutela dei dati personali nei diversi sistemi giuridici, gli utenti, con il loro consenso tramite un click sullo schermo del proprio interfaccia informatico, autorizzano spesso i fornitori di servizio a fare gli usi più vari e, per molti versi, imprevedibili di quei dati. È il caso occorso qualche anno fa in un popolare magazzino nordamericano a una teenager e alla sua famiglia, a cui gli addetti del magazzino riferirono che, stante le spese fatte e deducibili dagli scontrini, l'elaboratore elettronico della grande catena di vendite era giunto alla conclusione che, insomma, quella ragazzina fosse incinta. Sebbene neanche lei lo sapesse, tutti avrebbero poi appreso… ch'era vero!

D'altro canto, tra le tecniche usate dalle imprese per sfruttare il valore economico dei dati, basti pensare alla profilazione delle persone (*profiling*), e alle tecniche che, come il *data mining*, consentono di estrarre informazioni da un numero umanamente incomprensibile di dati (*big data*). Si tratta dei nuovi campi scientifici e tecnologici del sapere nati, e poi consolidatisi, solo all'inizio di questo secolo; e che dischiudono, nel bene e nel male, settori inediti per la sorveglianza. Possiamo sfruttare la conoscenza di gigantesche banche dati in settori come la ricerca medica, in rapporto ad esempio ai dati statistici sulla propensione o diffusione delle malattie estraibili, appunto, dall'ambito dei *big data*. Ma questi ultimi, insieme alle tracce digitali che ciascuno di noi lascia quotidianamente, possono essere sfruttati commercialmente per "farvi il profilo", o per vendere queste informazioni a terzi, perché a loro volta ne sfruttino il potenziale economico. La nuova sorveglianza che deriva dall'impiego delle tecnologie del *profiling* e *data mining*, va così a unirsi alle forme di autotutela delle imprese nel settore del copyright e con la protezione della proprietà intellettuale tramite tecniche DRM, sistemi di filtri e accessi controllati in rete, monitoraggio a distanza e altro ancora (v. § 5.4). Il risultato è una capacità di controllo sul comportamento e, forse, perfino sui pensieri e i desideri degli individui, senza precedenti. Come ebbe modo di dichiarare verso la fine del 2013, Stewart Baker, già consigliere generale dell'NSA, "i metadati ti dicono proprio tutto sulla vita di una persona. Se hai metadati a sufficienza, non c'è neanche bisogno di sapere il contenuto […] È perfino imbarazzante quanto prevedibili siamo come esseri umani" (in Cole 2014).

Il terzo protagonista della "nuova sorveglianza" è per ultimo, ma non da ultimo, "You". Il riferimento va sia alle nuove forme di controllo tra i privati, sia all'uso dei media come forma per tenere sotto controllo, in chiave di trasparenza, gli organi

pubblici. Nel primo caso, si tratta dell'esperienza quotidiana di poter controllare chi e con che ultimo accesso quel qualcuno sia presente in una rete come WhatsApp, se sia disponibile o occupato su Skype, e via dicendo. Ci sono software gratuiti per la geo-localizzazione e capire da dove una persona vi sta scrivendo o telefonando, così come la mania nell'uso dei droni, scoppiata negli Stati Uniti nel febbraio 2012, ha già portato all'impiego di queste macchine per spiare il comportamento delle proprie ex fidanzate. Tale forma di sorveglianza, per così dire, trasversale e obliqua, si è oltremodo diffusa anche in paesi come la Cina, ora al fine di denunciare e scovare l'individuo che si è macchiato di crimini odiosi, come nei casi di stupro, ora per denunciare e scovare politici o funzionari corrotti. Passando di qui al secondo caso di forme di controllo da parte dei privati ai fini della "nuova sorveglianza", è da ricordare come "dopo un disastro ferroviario dell'alta velocità nella città di Wenzhou nel luglio 2011, che uccise almeno 40 persone, ferendone circa 200, gli utenti cinesi d'internet cominciarono a usare i servizi di Weibo per twittare la diretta degli eventi e criticare la corruzione e abusi che avevano condotto al disastro" (MacKinnon 2012: 44).

In che senso, dunque, la sorveglianza condotta sia dagli stati nazionali, sia dalle imprese private, sia dai cittadini delle società ICT-dipendenti, è "nuova"? E che cosa accomuna queste forme così diverse di sorveglianza, volte, ora, ai fini condivisibili della sicurezza nazionale, dei servizi ottimali delle imprese o della denuncia dei cittadini; ora, invece, ai fini del controllo totale sulle comunicazioni, con lo scopo di profilare i propri clienti o per dar vita a nuove caccie alle streghe su internet?

Tirando le fila del discorso, si può dire che la sorveglianza nell'era delle società ICT-dipendenti è nuova, nel bene o nel male, per due ordini di ragioni. Rispetto alle forme tradizionali di sorveglianza, la rivoluzione informatica ha reso innanzitutto immanente all'agire quotidiano, il processo di raccolta e uso di dati che, automatizzato, risulta per ciò stesso continuo e onnipresente, disponibile in tempo (quasi) reale. In altri termini, la raccolta dei dati e delle informazioni non si presenta come un'attività separata dai comportamenti "naturali" di ogni giorno; ma, piuttosto, è interna a essi e, di qui, (quasi) invisibile, che si tratti dell'interazione su internet, oppure che essa avvenga nei luoghi fisici delle città, o tramite i propri telefoni cellulari.

Inoltre, la nuova sorveglianza appare più estensiva nel raggio di ampiezza della ricerca e più intensiva nella profondità dei dati analizzati, perché le nuove tecniche consentono di elaborare informazioni di tipo individuale – o attorno a categorie di dati e comportamenti con molteplici parametri di elaborazione – che, in definitiva, permettono di profilare una persona, ma anche d'incrociarne i diversi dati personali, al fine di prevederne il comportamento, da solo o a anche in rapporto a quello della sua rete sociale.

In molti sono giunti perciò alla conclusione che la privacy sia in realtà morta. Sarebbe del resto, questa, una conclusione per molti versi obbligata, vuoi che si tratti dello stato, vuoi delle imprese o del rapporto tra i privati, perché l'atto di osservare, di seguire con attenzione, qualcuno o qualcosa, è stato reso fisiologico e continuo, al fine di avere quel qualcosa o qualcuno sotto il proprio controllo, per prevenire o reprimere eventi non voluti, per garantire la normalità di una situazione, per sincerarsi del regolare svolgimento di un'attività, e via di questo passo.

L'invisibilità o, quantomeno, l'opacità che aveva tradizionalmente contraddistinto la vita delle persone, a contatto con le istituzioni o nel rapporto con gli altri indi-

vidui, si sarebbe alla fine dissolta, perché gli individui appaiono ora consenzienti, ora costretti o, addirittura, semplicemente ignari dei processi in corso.

Ma, stanno veramente così le cose?

### 6.2.3. *Morte della privacy?*

Rimane celebre la battuta di un noto CEO americano, Scott McNealy, allora capo della *Sun Microsystems*, che, tempo addietro, al momento del lancio di Jini, prodotto *wireless* potenzialmente in grado di riprendere tutti i movimenti dell'utente, dichiarava che con l'avvento delle nuove tecnologie avremmo semplicemente perso la nostra privacy: "You have zero privacy now. Get over it!".

La tesi sarebbe stata poi più volte ripresa, fino a diventare un motivo ricorrente e popolare dalla fine degli anni novanta: basti pensare al titolo di certi libri come *The End of Privacy* (Sykes 1999); o *The Death of Privacy* (Jarfinkel 2000); o *Privacy Lost* (Holtzmann 2006); ecc.

Ci sono, però, almeno tre modi diversi d'intendere la tesi che, pertanto, vanno tenuti distinti: il primo modo, cui si è fatto cenno con la battuta di McNealy, riporta all'impostazione, a noi nota, del tecno-determinismo (v. § 1.2). La tesi è che l'arsenale di mezzi tecnici come i sistemi di filtri usati in Occidente, o la grande muraglia digitale in Cina, con programmi per la raccolta di metadati, per via di GPS, CCTV, DNA, dati biometrici e ulteriori tracce e contenuti digitali di email, acquisti e prenotazioni in rete, carte di credito e operazioni bancarie, PayPal su eBay, DRM, prenotazioni di macchine o alberghi, il tutto poi raccolto in gigantesche banche dati, basti e avanzi a decretare un futuro già scritto, ossia, appunto, la morte della privacy.

Il secondo motivo per cui si afferma che la vecchia tutela della vita privata sia destinata a soccombere, è più sofisticato. Secondo questa variante raffinata del tecno-determinismo, si sostiene che, sebbene molti sistemi giuridici invochino la protezione della privacy con la tutela dei dati personali, la forza della tecnologia è tale da averne piegato le forze immunitarie sul piano delle garanzie nel campo della iurisdictio e dei controlli sugli organi di governo, come anche sul fronte delle norme sociali del kosmos, e come dimostra peraltro la mole degli scandali ricordati nelle pagine precedenti.

Infine, si può pensare che la privacy sia morta perché, semplicemente come suggerisce il fondatore di Facebook, Mark Zuckerberg (n. 1984), si tratta di un concetto vecchio e superato. L'idea che ciò che rende profonda la nostra vita debba rimanere in qualche modo nascosto sullo sfondo, sarebbe qualcosa di obsoleto, in quanto le coppie di opposizioni elementari tra visibile e invisibile, piatto e profondo, andrebbero ripensate al fine di rendere trasparente ciò che fin qui era rimasto opaco, in un nuovo tipo di interazione sociale che trova nella piattaforma sociale di Zuckerberg la sua espressione ideale.

Vediamo a continuazione quanto robuste siano queste tesi.

### 6.2.4. *Araba fenice*

Nell'antica mitologia egizia e greca, l'araba fenice era l'animale capace di risorgere dalle proprie ceneri, ogni volta che fosse stato dato per morto. Qui, l'immagine

sta a suggerire che, pure ad ammettere che la privacy sia morta, essa, nel frattempo, sarebbe risorta. Per capirne il perché, torniamo alla figura 19 di § 6.2, a proposito di processi cognitivi, tecniche e istituzioni della privacy nelle società ICT-dipendenti. Del secondo osservabile della figura, occorre ora approfondirne le tre variabili.

Innanzitutto, per ciò che concerne i processi cognitivi, è da concedere che le nuove tecniche della sorveglianza incidano profondamente sul modo in cui intendiamo tutelare la vita privata degli individui. La nuova sorveglianza è diventata immanente alla vita quotidiana e, per ciò stesso, invisibile, nel senso che appare poco controllabile, non appariscente o, perfino, fisiologica. A differenza, però, dei cultori della tesi sulla morte della privacy, bisogna pur aggiungere che, come esistono tecniche volte al monitoraggio e controllo degli individui, esistono anche tecniche protettive; vale a dire, tecniche il cui scopo principale è precisamente quello di preservare la privacy. Ad illustrare il punto, bastino per ora due esempi: il primo riguarda la crittografia, ossia la tecnica e i metodi per codificare e rendere illeggibili a terzi i contenuti delle trasmissioni, come nel caso dei protocolli SSH, SSL/TLS, HTTPS e IPsec nel transito tra client e server su internet, per la serie delle transazioni finanziarie o bancarie, per garantire la confidenzialità delle comunicazioni tra computer, con i cellulari, ecc. Il secondo esempio è dato dal principio della "privacy tramite design", il cui intento è d'immettere nel disegno dei prodotti, processi, luoghi o spazi dell'interazione degli individui, le norme disposte dal legislatore a tutela della loro vita privata. Si tratta di un principio, abbozzato fin dalla prima direttiva comunitaria per la protezione dei dati personali, cui abbiamo fatto cenno nel capitolo precedente (§ 5.5), e che è stato presentato dalla Commissione europea come cardine della propria proposta di nuovo regolamento nel gennaio 2012 (v. § 5.4.3).

La tensione che viene a darsi in questo modo tra tecnologie "pubblico-protettive" e "liberalizzanti" (Etzioni 2004: 45), non significa tuttavia che la tecnica sia in qualche modo neutra; quasi fosse il semplice strumento per raggiungere i fini più vari. Piuttosto, si arriva, anche per questa via, a quello scontro tra tecniche, disegnate appositamente per scopi differenti, che abbiamo illustrato nel capitolo scorso (§ 5.4.2). In quella sede, l'opposizione era data dai fini di proteggere o aggirare le difese a presidio dei prodotti posti sotto proprietà intellettuale; qui, invece, si tratta di proteggere o aggirare le tutele a presidio della vita privata tramite il design della tecnologia. Lungi dall'essere una questione risolvibile, essa stessa, per via tecnologica, ciò che lo scontro consiglia è di passare alla versione più sofisticata della tesi del tecno-determinismo: proprio perché disponiamo tanto di tecniche protettive, quanto di tecniche offensive, nei confronti della privacy, la tesi della sua morte deve spiegare come e perché le tecniche "pubblico-protettive" avrebbero alla fine prevalso. Ciò riconduce alla seconda variabile dell'indagine svolta in questo paragrafo, vale a dire le "tecniche" di cui alla figura 19.

Per prima cosa, occorre notare una volta di più come la tecnologia incida sulla tesi kelseniana del diritto come tecnica e, più in particolare, come mezzo del controllo sociale che si attua mediante la minaccia di misure coercitive: "se A, allora B" (v. § 1.4.3). La tensione tra tecnologie "liberalizzanti" e "pubblico-protettive" chiama infatti in causa, da un lato, l'insieme dei congegni, apparecchi o sistemi che consentono il flusso delle informazioni in reti fortemente decentrate, come quella d'internet, che mettono per ciò stesso in difficoltà il consueto apparato repressivo e sanzionatorio

degli stati. A questo dato, però, bisogna d'altro canto aggiungere la reazione di questi ultimi, nell'avvalersi dei più sofisticati dispositivi tecnologici "pubblico-protettivi" che, spesso, sono finanziati o messi a punto proprio dai laboratori delle agenzie di sicurezza degli stati nazionali. Gli scandali occorsi in tutti questi decenni, dal sistema di intelligenza sui segnali o *Echelon*, al programma Prisma dell'NSA (§ 5.4.3), starebbero in sostanza a segnalare come, alla fine, i dispositivi tecnologici "pubblico-protettivi" abbiano prevalso su quelli "liberalizzanti". Sia sul piano delle garanzie nel campo della iurisdictio e dei controlli sugli organi di governo, sia sul fronte delle norme sociali del kosmos, le forze immunitarie del sistema sarebbero in definitiva venute meno. Ma, appunto, stanno così le cose?

Per quanto concerne il primo fronte immunitario del sistema, abbiamo visto fin dal capitolo terzo (§ 3.2), che la formula kelseniana del diritto "se A, allora B" debba intendersi alla luce del dualismo tra gubernaculum e iurisdictio. Quest'ultima è infatti preposta al controllo di legalità, sia sul tenore delle decisioni politiche ("A"), sia sul fronte delle conseguenze pratiche ("B"). La totalità del sistema immunitario dell'ordinamento, ben inteso, non può, né deve, poggiare, sui soli organi della iurisdictio: sebbene, in alcuni grandi eventi della storia, come all'inizio del costituzionalismo inglese del primo Seicento, ciò possa accadere (v. §§ 3 e 3.1.1); più spesso, gli organi della iurisdictio non possono che intervenire a posteriori. È a quanto si è potuto assistere con le sentenze della Corte suprema americana sulla tecnologia P2P (§ 1.2), o sul *Communications Decency Act* (§ 3.4.1); oppure con le pronunce della Corte di giustizia sui diritti fondamentali (§ 4.3.2.1), a proposito di privacy e tutela della proprietà intellettuale con sistemi di filtraggio (§ 5.4.3), o marchi e brevetti (§ 4.3.3.2); per giungere all'Opinione della Corte distrettuale della Columbia, il 16 dicembre 2013, nel caso *Klayman vs. Obama* (§ 5.4.3).

Ciò che questa serie nutrita d'interventi giudiziari, e molti altri che esamineremo in tema di privacy nel corso dei prossimi capitoli, sta in definitiva a segnalare è che le voci sulla morte o fine dell'istituto sono infondate perché, anche ad ammettere che il paziente sia veramente grave, come suggeriscono in fondo alcune delle sentenze ora riportate, esso è ben lungi dall'esser morto nelle aule giudiziarie. Altrimenti, in tutta questa pletora di casi, di cosa staremmo mai discutendo?

L'interrogativo conduce al secondo fronte immunitario del sistema e, di qui, all'ultima serie di argomenti per sostenere la fine della privacy. Le opposizioni elementari di visibile e invisibile, piatto e profondo, secondo quest'ulteriore prospettiva, andrebbero infatti ripensate nel senso di come rendere trasparente ciò che fin qui era rimasto opaco, avendo a che fare con un concetto, quello di privacy, che poco o nulla importerebbe alla nuova generazione di nativi o naturalizzati digitali. Si tratta della tesi pontificata dal capo di Facebook che, sul piano filosofico, riconduce ai paradossi della privacy come "controllo" (v. figura 18). Anche a riferire tutti i dati della propria vita, questa scelta, se fondata sul consenso, non priverebbe gli individui della loro privacy, perché in ogni modo essi avrebbero optato per simile condizione di totale trasparenza. È una considerazione che, in fondo, vale anche per il concetto di sorveglianza sul quale siamo venuti discorrendo in queste pagine, che si presta tanto a un significato positivo come a uno negativo: possiamo in realtà giustificare molti casi in cui è indispensabile osservare, o seguire con attenzione, qualcuno o qualcosa, per prevenire o reprimere eventi non voluti, o sincerarci del regolare

svolgersi di un'attività, la quale deve per ciò stesso diventare del tutto cristallina a chi osserva o sorveglia.

Lasciando da parte i profili normativi ed etici della questione – con i temi del design e i rischi di paternalismo (§ 5.3.3) – è tuttavia da dimostrare che alle nuove generazioni di nativi digitali, come a quella dei naturalizzati, nulla importi della propria privacy: molte inchieste e ricerche statistiche stanno a mostrare il contrario[2].

Inoltre, per evitare indebite generalizzazioni (si v. § 6.2), sarebbe non solo il caso di specificare il tipo di privacy (v. figura 18), ma anche a quale livello e all'interno di quale contesto culturale se ne parla.

Si tratta dell'ulteriore variabile della figura 19, definita dal profilo delle istituzioni, che occorre approfondire con gli osservabili della tavola 6 illustrata nel capitolo quarto (§ 4.3.3.2). Bisogna, cioè, chiarire il contesto del quale si discute, attraverso i parametri nazionali, internazionali e transnazionali della ricerca e in rapporto alla forza che le leggi, il mercato e le norme sociali del kosmos hanno in quel contesto determinato. Basti far cenno alle differenti aspettative di privacy che, pur esistono, tra orientali e occidentali; e, allo stesso modo, come anche tra questi ultimi, tra italiani e svedesi, nordamericani e tedeschi, permangano rilevanti differenze. Per uno svedese, ad esempio, sarebbe del tutto naturale ciò che tanto scandalo, invece, provocò in Italia con la scelta compiuta dal ministro delle finanze di mettere in rete, a disposizione del pubblico, la lista dei redditi dei contribuenti 2008. Del pari, sarebbe strano osservare in Italia la minuziosa tutela della privacy che può riguardare la protesta di massa in Germania, contro le riprese e le foto di Google per i servizi di mappe (*maps*) e di vie (*street*).

Senza dover recare altri esempi, l'idea dovrebbe però essere chiara: la tesi sulla morte della privacy è una semplificazione giornalistica che pure ha avuto discreto successo, proprio perché riesce a sintetizzare il senso di spaesamento provocato dalla trasformazione tecnologica del diritto. Alla differenziazione nazionale e generazionale dei problemi qui affrontati, occorrerebbe peraltro aggiungere la dimensione internazionale e transnazionale di questi stessi problemi che, qualche anno fa, erano per lo più riassunti con la formula della "globalizzazione giuridica". Sul piano istituzionale, il rinvio si riferisce alla pletora di documenti, leggi o accordi internazionali, che sono venuti accumulandosi sul punto, per il tramite del lavoro di enti come l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), le Nazioni Unite o l'Unione europea. La ragione di questo impegno è del resto evidente, non appena si ricordi come molti dei temi discussi a proposito di privacy mediante le tecnologie "pubblico-protettive" confermino che i tradizionali confini giuridici degli stati nazionali sono attraversati da sistemi di intelligence sui segnali all'estero, con programmi di filtraggio per il flusso delle informazioni in rete, che a loro volta possono essere controllati da dispositivi DRM, sistemi per l'ispezione in profondità dei dati trasmessi su internet (*deep packet inspection*), e altro ancora.

Vediamo dunque a continuazione come la tecnologia abbia riplasmato il vecchio istituto della privacy, privilegiando il piano istituzionale, rispetto ai meccanismi cognitivi e alle tecniche, del diritto.

---

[2] Si v. ad esempio *http://europa.eu/rapid/press-release_MEMO-14-186_en.htm*.

## 6.3. *Globalizzazione giuridica*

I temi della globalizzazione giuridica consigliano di far ritorno alle 30 variabili della tavola 6 in § 4.3.3.2. Un modo per ordinarne lo studio e stabilirvi le convenienti priorità, è dato dall'asse orizzontale della tavola, onde esaminare le scelte del gubernaculum, le decisioni della iurisdictio, la meccanica dei contratti e l'evoluzione delle norme sociali, dal punto di vista, rispettivamente, del diritto transnazionale, internazionale e nazionale della privacy. Partiamo dunque con l'analisi delle tre ultime variabili messe in mostra dalla figura 19, in chiave transnazionale (§ 6.3.1), e internazionale (§ 6.3.2), mentre il piano nazionale (§ 6.3.3) servirà a introdurre il prossimo capitolo sul modello nordamericano della privacy.

### 6.3.1. *Privacy transnazionale*

Il piano transnazionale della privacy è per molti versi quello con cui il lettore ha maggiore dimestichezza: sono i nostri rapporti con la galassia dei servizi internet o sul web offerti dai loro fornitori (ISP). Di questo piano occorre menzionare tre ulteriori sotto-variabili che concernono i termini del rapporto tra ISP e utenti, la relazione tra diritto transnazionale e gli organi del gubernaculum, soprattutto sul piano del diritto nazionale con, infine, le annesse questioni di giurisdizione che detta relazione presenta.

Innanzitutto, i rapporti tra ISP e utenti sono per lo più regolati sulla base del consenso prestato dagli individui ai termini del servizio di quel fornitore. La prima sotto-variabile che occorre pertanto richiamare riguarda, ora, l'accordo tra le parti con la tecnica dell'"opt in" (§ 5.3), ora, il loro eventuale scontro, come già occorso con il caso di Facebook (§ 5.1.3). Questa dimensione transnazionale dei temi della privacy è peraltro favorita dall'approccio statunitense che privilegia l'auto-regolamentazione e concorrenza tra le forze del mercato. Ciò non significa che anche negli USA, come in Europa, gli attori del mercato non entrino a contatto con gli organi statali, più che internazionali, del gubernaculum e della iurisdictio, come del resto esemplificato dalle richieste di dati e informazioni agli ISP, da parte delle autorità nazionali, ai fini della sicurezza o ordine pubblico (§§ 6.2.1 e 6.2.2). La circostanza introduce il secondo ordine di sotto-variabili alle quali si deve qui far cenno.

Infatti, sebbene ci sia spesso un rapporto di collaborazione, o anche convenienza reciproca, non sono mancati i casi di aperto contrasto tra diritto nazionale e diritto transnazionale, tra gubernaculum e consigli di amministrazione delle grandi società del settore. A volte, sono queste ultime imprese a essere tenute, volenti o nolenti, al rispetto delle regole fissate dal legislatore nazionale (§ 4.3.3.2). Altre volte, però, sono esse, più che lo stato, a tutelare la privacy dei propri clienti, o utenti, nel rispetto dei diritti dei cittadini di uno stato determinato. Per prendere come esempio Google, così, nel 2006, a differenza di alcune concorrenti come *American on Line* o *Yahoo!*, la società californiana non ha ceduto alla richiesta e pressioni del Dipartimento di giustizia nordamericano di mettere a disposizione del governo un campione a caso delle parole chiave più ricercate nel corso di una settimana dagli utenti, oltre a un milione di siti Web scelti senza speciali criteri dall'indice del motore (la richiesta del presidente George W. Bush era formalmente giustificata dai fini della lotta alla

pornografia in rete). Nel 2010, in risposta questa volta agli attacchi informatici subiti sotto pressione del governo cinese per censurare le ricerche dei propri cittadini attraverso il popolare motore di ricerca, Google ha poi deciso di dirottare il flusso delle richieste sui propri server a Hong Kong e, dunque, sotto una giurisdizione sottratta alle pretese del governo di Pechino.

Sempre l'esempio di Google introduce la terza serie di sotto-variabili dell'esame sul rapporto tra diritto transnazionale e nazionale, questa volta sul fronte della iurisdictio. Sebbene Google abbia spesso reclamato nel corso dell'ultimo decennio, specie nei confronti delle autorità giudiziarie in Europa, che la propria attività di raccolta e trattamento dei dati personali non va sottoposta alle loro giurisdizioni, essendo svolta quella attività, appunto, fuori dall'Europa, la società californiana è stata chiamata più volte a rispondere, all'atto pratico, del suo comportamento davanti a quei giudici nazionali. Un caso lampante, sia pure favorevole a Google, si è avuto con il processo noto come *Vividown*. Con la decisione 1972 del 24 febbraio 2010, il tribunale di Milano aveva infatti condannato alcuni funzionari della società californiana per "trattamento illecito dei dati personali", ai sensi dell'articolo 167 del codice italiano sulla privacy, avendo permesso che un video, nel mostrare un fanciullo autistico nell'atto di essere molestato e sbeffeggiato dai compagni di scuola, fosse da questi ultimi caricato sulla piattaforma per video di Google. Per motivi più convincenti (Pagallo 2009; Sartor e al. 2010; ecc.), la sentenza sarebbe stata riformata: prima la Corte d'appello di Milano e, poi, la Corte di cassazione nel 2013, hanno assolto gli imputati per non aver commesso il fatto. Nonostante valga, anche nel caso di Google, l'adagio per cui tutto è bene ciò che finisce bene, l'esempio serve a chiarire come il fronte nazionale della iurisdictio possa interferire con l'attività transnazionale di raccolta e trattamento dei dati da parte degli ISP più importanti.

### 6.3.2. *Privacy internazionale*

Abbiamo riferito nelle pagine precedenti l'apporto del diritto internazionale della privacy tanto sul piano della iurisdictio, quanto su quello del gubernaculum. Nel primo caso, si pensi alla giurisprudenza della CEDU in tema di privacy e sicurezza nazionale (v. § 5.4.3); nel secondo caso, il riferimento va alla Dichiarazione universale del 1948 e alla Convenzione europea del 1950, ricordate nell'introduzione del presente capitolo. Oltre agli accordi o trattati internazionali multilaterali, vanno naturalmente aggiunti quelli bilaterali, come nel caso degli accordi tra USA e UE sul fronte dei dati trattati nell'ambito del trasporto aereo, o per quanto concerne le pratiche "leali" di trattamento nel campo commerciale, su cui torneremo (v. §§ 8.4.4 e 9.1).

A queste variabili della privacy internazionale si affiancano, poi, le forme del diritto soffice (§ 4.3.3.1): se, nel capitolo quarto, l'esempio era fornito dalle autorità del diritto nazionale nel settore della protezione dei dati, qui, il punto può essere illustrato con il documento rilasciato l'11 settembre 2014, dall'Alto Commissario per i diritti umani presso le Nazioni Unite (ONU), in cui, assodato che il diritto alla privacy è protetto sia dalla Dichiarazione universale che dalla Convenzione internazionale sui diritti civili e politici, si sottolineano tuttavia le nuove sfide della sorveglianza elettronica, per le quali gli stati nazionali dovrebbero adottare "un quadro normativo chiaro, preciso, accessibile, comprensivo e non discriminatorio, al fine di

regolare tutte le attività di sorveglianza condotte dalle forze dell'ordine e le agenzie di sicurezza" (§ 50 del documento). In particolare, i principi ispiratori dell'intervento dovrebbero essere quelli di "legalità, necessità e proporzionalità" (*op. cit.*, § 23); e "gli stati dovrebbero garantire un controllo e rimedi effettivi per le violazioni della privacy a mezzo della sorveglianza digitale" (§§ 37-41). Stante la complessità e velocità delle trasformazioni in corso, l'Alto Commissario ha poi sottolineato la necessità di "ulteriori discussioni e studi approfonditi sui problemi relativi all'effettiva protezione della legge, con garanzie processuali, controlli effettivi e rimedi" (§ 51), che a loro volta richiedono il comportamento responsabile degli attori privati e nel settore commerciale, nonché il coinvolgimento di tutte le organizzazioni non governative (NGO), volte alla difesa della privacy. Tra queste, si sono da subito schierate con l'Alto Commissario, l'Osservatorio internazionale per i diritti umani (*Human Rights Watch*), l'ACLU, Amnesty International, l'EFF, *Privacy International*, e altre ancora.

Eppure, il quadro della privacy internazionale sarebbe affatto incompleto senza il diritto soffice dell'Organizzazione per la cooperazione e lo sviluppo economico, ente internazionale fondato nel 1948, che comprende buona parte dei paesi appartenenti alle democrazie in occidente. Infatti, nel 1980, l'OCSE ha pubblicato le Linee guida per la protezione della privacy e il flusso transfrontaliero dei dati personali (primo ottobre: C 58); che, riassunte nei dieci principi del documento, hanno orientato le politiche di protezione dei dati seguite negli anni a venire da molti stati democratici occidentali. I principi riguardano la raccolta limitata dei dati, la loro qualità, la specificazione dei fini del trattamento, i limiti del loro uso, le misure di sicurezza, l'apertura e la partecipazione individuale al trattamento dei dati, fino alle responsabilità giuridiche per l'uso e trattamento dei dati medesimi. Tra gli ordinamenti che si sono ispirati a questi principi, rendendo vincolanti e propriamente coattive le norme soffici dell'OCSE, è il caso di ricordare la disciplina comunitaria basata sul modello della "informativa e consenso". Sia pure temperata dalle relative eccezioni, la legittimità del trattamento dei dati nell'UE fa leva sul diritto che l'individuo ha di essere adeguatamente informato da parte del responsabile del trattamento circa i dati raccolti, la finalità del trattamento e i limiti all'uso dei dati, al fine di prestare il proprio consenso (art. 7 D-95/46/CE).

Tuttavia, nel richiamare la direttiva comunitaria 46 del '95, l'intento non è di aderire in questo modo alla tesi del Tribunale costituzionale tedesco, per il quale l'Unione europea e il suo diritto apparterrebbero alla sfera del diritto internazionale tradizionale (v. § 4.3.2.1). Quanto meno nell'ambito del trattamento e della tutela dei dati personali, occorre piuttosto avvertire come la normativa comunitaria si atteggi per molti versi, all'atto pratico, come un vero e proprio ordinamento di stampo federale. Al fine di metterlo a confronto con un ordinamento indiscutibilmente federale, come quello degli USA, per questo motivo, nel paragrafo seguente, passeremo in rassegna la serie di direttive che il Parlamento e il Consiglio europeo sono venuti approvando in materia. Nell'illustrare ciò che fuoriesce dalla competenza quasi-federale dell'Unione, dovremo, in fondo e in ogni caso, parlare del diritto nazionale dei suoi stati membri.

### 6.3.3. *Privacy nazionale*

L'ultima variabile dell'analisi, incentrata sulla figura 19 del § 6.2, concerne il piano nazionale relativo alla tutela della privacy e dei dati personali. Nonostante il ruolo che il diritto internazionale e transnazionale svolge in questo settore dell'ordinamento, occorre insistere sulle differenti culture, valori e tradizioni giuridiche in gioco, e sul diverso modo in cui i rapporti tra le leggi del gubernaculum, le decisioni della iurisdictio, i contratti del mercato e le norme sociali sono intesi nei sistemi giuridici di riferimento. Se, come detto (§§ 6.1.2 e 6.2.2), negli Stati Uniti d'America si privilegia l'auto-regolamentazione e la concorrenza, in Europa, invece, è prevalsa l'idea che tanto il gubernaculum, quanto la iurisdictio, fissino i principi entro cui concepire la dinamica giuridica del kosmos. È questo il filo conduttore che ispira la normativa europea in materia, a partire dalla più volte ricordata direttiva 46 del 1995, alla 58 del 2002, fino alla direttiva 24 del 2006, relativa agli obblighi dei fornitori di servizi nel campo della comunicazione elettronica accessibile al pubblico[3].

Alla luce di questa normativa, con buona pace del Tribunale costituzionale tedesco, occorre ribadire come la disciplina vigente in Europa assomigli al modo in cui funziona un sistema giuridico di tipo federale: § 4.3.2.1. Il legislatore di Bruxelles fissa, infatti, i principi e le condizioni, anche dettagliate, di legittimità delle normative nazionali, che gli ordinamenti degli stati membri sono tenuti a rispettare. Sebbene, a differenza dei regolamenti, le direttive lascino agli stati nazionali un margine di discrezionalità più o meno ampio, vige pur sempre il "primato del diritto comunitario" (v. § 3.2.2). Questo vuol dire che, in caso di contrasto con la normativa europea, gli organi della iurisdictio, in ogni stato membro, devono dirimere le controversie sulla base delle norme sovraordinate fissate a Bruxelles e, nel caso persistessero dubbi, è loro potere rinviare pregiudizialmente gli atti in Lussemburgo, presso la Corte di giustizia, affinché questa, come organo di chiusura, indichi come interpretare i trattati e le disposizioni del diritto comunitario. Quest'ultimo, a tutti gli effetti, funge così da parametro di legittimità della normativa nazionale.

Eppure, ci sono due differenze fondamentali con altri tipi di sistema federale come, ad esempio, quello nordamericano. Il primo punto riguarda le conseguenze, sul piano istituzionale, del diverso approccio auto-regolativo, o per principi, dei due sistemi: negli Stati Uniti, per dirla con la Corte suprema di Washington, "la protezione del diritto generale delle persone alla privacy [è] in buona parte lasciato al diritto dei singoli Stati [dell'Unione]"[4]. Al contrario, in Europa, è Bruxelles che fissa in buona parte quei principi nel campo della protezione dei dati: ne è conferma quanto affermano le autorità garanti (WP 29), in un documento del 2009 sul "futuro della privacy" (doc. WP 168), per cui l'idea è che occorra riformare la direttiva vigente, la D-95/46/CE, con un nuovo intervento che risolva gli attuali problemi di armonizzazione. Ancora oggi, in fondo, alcuni stati membri non hanno recepito il principio della risarcibilità per violazione della privacy informazionale, come ap-

[3] Torneremo sulla direttiva 24 nel capitolo ottavo (§ 8.4.4.1), a proposito della sentenza con cui, l'8 aprile 2014, la Corte di giustizia ne ha dichiarato l'invalidità.

[4] Il riferimento è al caso *Katz vs. U.S.*, 389 U.S. 347 (1967), su cui torneremo nel prossimo capitolo. La cit. in *op. cit.*, pp. 350-51.

punto stabilito dalla direttiva 46, oppure non hanno implementato le disposizioni relative alla responsabilità di chi tratta i dati. È quindi in questa direzione che si coglie perché la Commissione, nel proporre le riforme al settore nel gennaio 2012, non solo abbia accolto molti dei suggerimenti di WP 29, ma ne abbia dato la forma di regolamento, e non più di semplice direttiva.

La seconda differenza tra i modelli americano ed europeo ruota attorno al diverso modo in cui sono disciplinati i rapporti tra i privati o, per converso, tra individui e stato ai fini della sicurezza. Nel modello americano, quest'ultimo rapporto tra individuo e governo (gubernaculum) è disciplinato sul piano costituzionale federale: come diremo, i gravi problemi emersi negli ultimi tempi con le attività dell'NSA, o dell'FBI (§ 6.2.1), devono ricondursi alla protezione offerta dal primo e, soprattutto, dal quarto emendamento alla Costituzione. Per trovare invece, nel modello americano, la disciplina dei rapporti tra governo locale, sia pure statale, e individui, nonché tra questi ultimi con casi di responsabilità civile, bisogna passare al piano della legislazione di ogni stato membro dell'Unione: la California, il Texas, il Missouri, ecc. In questo senso, dunque, la Corte suprema nel caso Katz ha potuto dichiarare che "buona parte" è lasciato "ai diritti degli Stati". Si tratta di quell'immensa parte della legislazione, cui si affianca il common law giurisprudenziale che, oltre a un incipiente diritto amministrativo, trova ordine nella classica quadripartizione proposta da William Prosser (1898-1972). Di qui che, parlando di violazione della privacy negli USA, occorra quanto meno distinguere tra casi di responsabilità civile per appropriazione indebita, per intrusione, per diffusione di fatti privati o loro distorsione sotto "falsa luce" (Prosser 1960: 383).

Al contrario, per il modo e le ragioni in cui è venuta prendendo forma l'Unione europea, i rapporti tra i privati o, per converso, tra individui e stato ai fini della sicurezza, sono disciplinati in modo speculare a quello ora visto: i rapporti tra la privacy degli individui e la sicurezza dello stato sono gelosamente custoditi dagli stati membri dell'Unione in nome della loro sovranità. Nonostante le accresciute competenze dell'Unione, "buona parte" della partita si gioca sul piano del diritto nazionale e, in ultima istanza, con le competenze, sul piano internazionale, della Corte di Strasburgo in tema di diritti umani (§ 5.4.3). Viceversa, le direttive comunitarie in tema di trattamento e protezione dati hanno a che fare, soprattutto, con la disciplina del rapporto tra privati; o, quanto meno, introducono come sistematica eccezione alle regole generali del sistema, il rapporto tra privati e organismi pubblici dello stato, per determinare la legittimità del trattamento e uso dei dati personali. La ragione di questa diversa impostazione è dipesa dal bilanciamento tra i poteri sovrani degli stati e l'esigenza di favorire lo sviluppo di un mercato unico in Europa, con la libera circolazione delle merci, capitali, servizi e persone, a cui, a metà degli anni novanta del secolo scorso, è andata ad aggiungersi la necessità di regolare la libera circolazione dei dati e delle informazioni. Sebbene il diritto comunitario, a partire dagli anni settanta, sia stato progressivamente integrato con la tutela dei diritti umani, per giungere alla Carta di Nizza del 2000 e al trattato di Lisbona del 2009, anche dopo quest'ultimo accordo il rapporto tra sicurezza nazionale, diritti umani e privacy rimane sottratto alla "vocazione generale" del legislatore di Bruxelles. Ciò è confermato dalla proposta della Commissione di un nuovo regolamento per la materia, per cui all'articolo 2 ritroviamo il disposto del vecchio articolo 3, nel senso che "le

disposizioni del presente regolamento non si applicano ai trattamenti di dati personali […] effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, concernenti in particolare la sicurezza nazionale".

Queste differenze, anche radicali, tra gli ordinamenti portano non di rado con sé veri e propri malintesi tra giuristi di aree differenti, come il common law statunitense e il nuovo diritto comune europeo, oppure, anche tra giuristi di quest'ultima area, come, ad esempio, per il modo in cui la privacy viene tuttora percepita in Gran Bretagna a differenza, poniamo, dell'Italia, o in Germania. L'avvertenza sul ruolo che le specificità nazionali hanno, anche in rapporto ai temi della privacy come esempio di globalizzazione giuridica, servono per ciò a prevenire indebite generalizzazioni. Bisogna infatti cogliere come il riposizionamento tecnologico della privacy abbia preso forme diverse nei distinti ordinamenti, anche se, tanto al di là che al di qua dell'Atlantico, è dato scorgere e comparare due modelli: quello, appunto, invalso negli USA e quello che, invece, è venuto prendendo piede in Europa negli ultimi vent'anni.

Alla luce di una nuova figura, l'ultima di questo capitolo (figura 20), proviamo a riepilogare le tappe percorse in questa parte del libro; vale a dire, dal modo in cui, muovendo dal rapporto tormentato tra privacy e sicurezza (§ 6.2), l'indagine è passata ai profili cognitivi e tecnici della privacy nelle società ICT-dipendenti (§ 6.2.4), restringendo via via il fuoco dell'analisi sui profili strettamente giuridici del tema (§ 6.3), per cominciare a cogliere l'importanza che le diverse tradizioni nazionali, culture o valori, hanno per la tutela del diritto. Nell'apprestarci a esaminare come funzioni il diritto alla privacy negli Stati Uniti, occorre prevenire un ultimo fraintendimento.

La figura 20 che conclude il capitolo deve essere interpretata in modo tale che le considerazioni che faremo sulla particolarità del modello americano non escludano, bensì integrino, quanto detto finora sul riposizionamento tecnologico della privacy, ossia con i nuovi processi cognitivi e tecniche delle società ICT-dipendenti, e con i dilemmi che si danno tanto sul piano del diritto transnazionale, quanto di quello internazionale.

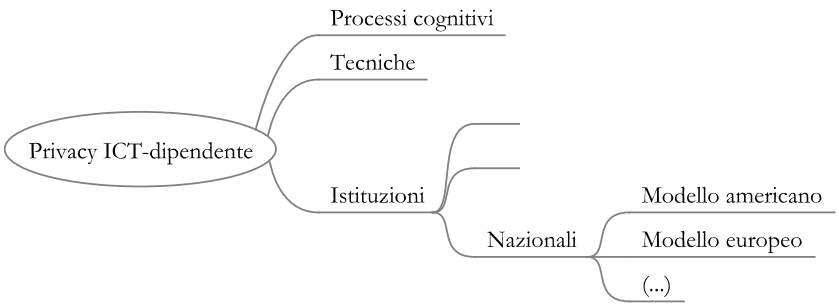


Figura 20: *Globalizzazione giuridica e tutela nazionale della privacy*

Con questa avvertenza, possiamo dunque procedere a considerare il diritto nazionale statunitense.

# VII.
# *Mr. Katz*

> "Colui che occupa la cabina, chiude la porta dietro di sé e paga il gettone che gli consente di fare la chiamata, è sicuramente autorizzato a credere che le parole dette durante la telefonata non saranno diffuse nel mondo. Leggere in maniera più ristretta la Costituzione significa ignorare il ruolo vitale che il telefono pubblico ha finito per avere nelle comunicazioni private"
>
> Justice STEWART

Il diritto alla privacy negli Stati Uniti d'America è un apparente coacervo di leggi, statali e federali, di sentenze e di condizioni contrattuali, di responsabilità penale e civile, che coinvolge e accomuna cose e casi così diversi, come la sfera civica della democrazia e il comportamento pubblico degli individui, la tutela del diritto di associazione per scopi politici e il diritto affinché quelle associazioni rimangano private, il diritto di cronaca e quello alla quiete, l'aborto e i rapporti tra omosessuali, la relazione tra due o più estranei o quella tra sposi, dove uno di essi può talora essere escluso dall'altro per coinvolgere un medico, e via dicendo. Per cominciare a orientarci in questa fitta rete di disposizioni normative, principi costituzionali, precedenti giurisprudenziali, termini contrattuali delle imprese e norme sociali dal contenuto più vario, limitiamoci per intanto a soffermare la nostra attenzione sul rapporto, a noi ben noto, tra gubernaculum e iurisdictio.

Riprendendo idealmente una variabile della figura 20, con cui si è chiuso il capitolo precedente, possiamo illustrare i nuovi osservabili e variabili dell'analisi con un'altra figura, la 21, che il lettore trova qui sotto, a pagina 194.

Anche a non tenere per ora in conto il kosmos, sia sul fronte dell'autonomia contrattuale delle parti sia per quanto riguarda il ruolo svolto dalle norme sociali, la figura 21 mette bene in mostra la complessità del nostro tema.

Partendo dal gubernaculum sul piano federale, lo schema attira l'attenzione, in primo luogo, sul susseguirsi di norme e statuti approvati dal Congresso di Washington in materia. Per comodità, la figura li divide in due gruppi: gli interventi legislativi in tema di sicurezza nazionale che abbiamo esaminato nel capitolo precedente (§ 6.2.1); e la pletora di leggi con cui, volta per volta, il Congresso è intervenuto a disciplinare i settori più vari, a proposito del furto d'identità digitali, video voyeurismo, accesso ai documenti del governo, tutela dei dati sanitari e nel campo assicurativo, registri della motorizzazione, ecc. (si v. § 6.1.2). Non sorprenderà che si conti-

no sulle dita di una mano i giuristi americani che si occupano di privacy *tout court* e, al contrario, che la maggioranza finisca per specializzarsi su privacy sanitaria, privacy in luoghi pubblici, privacy su internet, ecc.

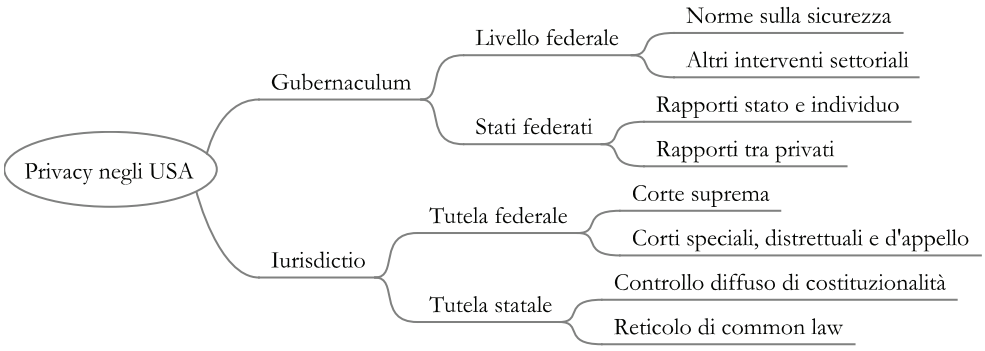


Figura 21: *La tutela della vita privata negli USA tra gubernaculum e iurisdictio*

D'altra parte, si tratta di una materia che, negli Stati Uniti d'America, per dirla ancora con la Corte suprema (§ 6.3.3), è "in buona parte" lasciata agli Stati dell'Unione: insieme alle norme che disciplinano il rapporto di ciascuno dei cinquanta stati con la propria popolazione, la legislazione ordinaria ha soprattutto a che fare con l'ambito delle relazioni tra privati cittadini e associazioni. All'accennata specializzazione per materia si affianca, così, la difficoltà di dover fare i conti con cinquanta diversi regimi sulla privacy, che conducono a differenze di tutela anche notevoli all'interno della Unione tra, poniamo, la California e l'Alabama. L'attivismo degli stati incontra comunque il limite di non poter restringere in forma indebita, l'altrui sfera, costituzionalmente protetta, della privacy. Ad esempio, nel caso *Boy Scouts of America vs. Dale* del 2000, la Corte suprema ha dichiarato l'illegittimità costituzionale della legge [*statute*] di uno Stato dell'Unione che, al fine di promuovere gli interessi delle associazioni omosessuali, finiva per restringere indebitamente la privacy e i diritti associativi dei Boy Scout [1].

Passando al fronte della iurisdictio, anche qui, ovviamente, conviene distinguere i piani federale e dei singoli stati. Nel primo caso, troviamo tanto la Corte suprema, quanto i tribunali minori, sebbene alcune decisioni delle corti federali distrettuali o delle corti d'appello possano avere notevole rilievo. Nel secondo caso, invece, ritroviamo tanto il meccanismo del sindacato diffuso di costituzionalità delle leggi (§ 3.2 (iii)); quanto la tutela che, nei termini del civil law europeo, verrebbe associata alla sfera del diritto privato e della responsabilità extra-contrattuale. Riprendendo la quadripartizione di Prosser, si tratta della variegata tutela che il common law offre per appropriazione indebita, intrusione, diffusione di fatti privati o loro distorsione sotto "falsa luce" (v. § 6.3.3).

Come detto, la figura 21 lascia fuori le forze del kosmos: innanzitutto, una parte

[1] 530 U.S. 640 (2000).

considerevole della tutela in tema di privacy negli Stati Uniti è affidata alla concorrenza del mercato e all'auto-regolamentazione dei suoi attori tramite codici di autocondotta, termini di servizio e programmi di conformità a dette regole. Sono rari i casi in cui le autorità federali hanno perseguito compagnie private, ree di non aver ottemperato alle proprie obbligazioni: tra i pochi, questo è quanto occorso a Geocities nel 1999. Ciò non significa ovviamente che le compagnie private siano state integerrime nel corso di tutti questi decenni; ma, piuttosto, segnala un approccio libertario, o liberista, a seconda della prospettiva e dei problemi presi in considerazione, in tema di privacy in America.

Inoltre, manca nella figura 21 il ruolo che le norme sociali giocano in questo caso e che, come diremo nel corso del capitolo, è determinante. Davanti alla folla di settori e argomenti trattati negli USA sotto l'etichetta della privacy, che hanno condotto a una specializzazione ora settoriale, ora per stati dell'unione, tornano utili le parole del collega di Georgetown, Charles Abernathy (n. 1946): "l'insieme di concetti etichettati come privacy è assai più interessante se considerato come riflesso e cifra della cultura e dei valori americani, un insieme, cioè, di valori e scelte dominanti ancorché incoerenti che riflettono le tendenze sulle appropriate regolazioni sociali" (in Pagallo 2008: 68). Dal punto di vista del diritto costituzionale, è significativo che la Corte suprema, nel corso degli ultimi decenni, sia infatti venuta ragionando, e decidendo, in tema di privacy, sulla base di una (soggettiva e oggettiva) "ragionevole aspettativa", e cioè di ciò che, ora una singola persona, ora la società in quanto tale, si aspetta rimanga ragionevolmente in privato. Sebbene il diavolo sia nei dettagli, e possa essere difficile stabilire in concreto le norme sociali che rendono ragionevole aspettarsi il riserbo del governo e degli altri, su cui si fonda in molti casi il diritto alla privacy negli USA, appare chiaro come le norme sociali svolgano un ruolo di prim'ordine in questo sistema giuridico.

Per approfondire la questione che, poi, costituisce il filo conduttore del presente capitolo, bisogna concentrare l'attenzione su una precisa variabile della figura 21: la Corte suprema. Più in particolar modo, avendo presente la sua giurisprudenza, sarà il caso di restringere ulteriormente il campo della nostra disamina, e considerare soltanto quella parte del *case law* (i precedenti) della Corte che concernono la tutela del primo e quarto emendamento alla costituzione americana (v. § 3.1.3.1). Il primo di essi è stato già ricordato (§ 3.4.1); ma, per comodità e importanza, ne riporto ancora una parte: "Il Congresso non potrà fare leggi […] per limitare la libertà di parola, o di stampa; o del diritto del popolo di riunirsi pacificamente". Il quarto emendamento, invece, recita che "non potrà essere violato il diritto del popolo di avere sicurezza per le proprie persone, abitazioni, documenti ed effetti, contro ogni irragionevole perquisizione o sequestro".

Su queste basi, per capire alcuni aspetti cruciali su come funzioni e sia teorizzata la privacy negli Stati Uniti, tra le decisioni politiche del gubernaculum con le sue leggi, i contro-poteri della iurisdictio, l'autonomia delle forze private in forza di contratti e la ragionevole aspettativa che la riservatezza delle persone sia rispettata in omaggio alle norme e consuetudini sociali, il presente capitolo è presentato in cinque parti. Esse sono introdotte con una nuova figura che mostra gli osservabili e variabili del nuovo livello d'astrazione:

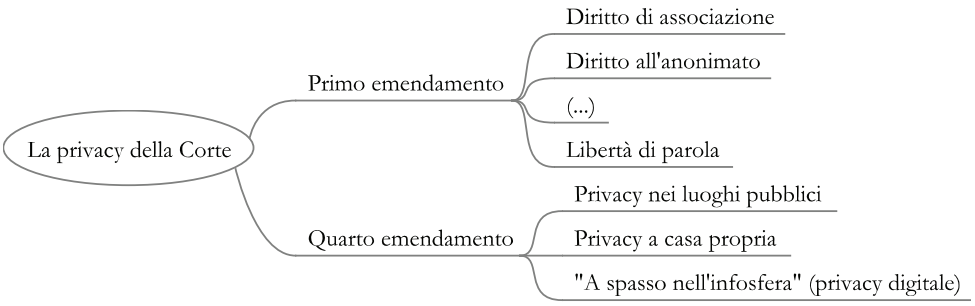


Figura 22: *Libertà di parola e quarto emendamento nella giurisprudenza della Corte suprema*

A continuazione (§ 7.1), l'attenzione sarà incentrata sulla privacy in rapporto alla tutela del primo emendamento nell'interpretazione della Corte suprema: sebbene questa tutela comprenda i problemi legati al diritto di associazione e di anonimato, il paragrafo sarà dedicato alla "libertà di parola" (*freedom of speech*). Questo diritto è bilanciato dall'altrui diritto a essere lasciato indisturbato; ma, a differenza dell'Europa, la libertà di parola si atteggia, quasi all'inverosimile, come un diritto semi-assoluto.

Dopo di che (§ 7.2), ci occuperemo della tutela accordata alla privacy in rapporto al quarto emendamento: su di esso, in fondo, si basano tutti i diritti esaminati nel resto del capitolo. Sia per motivi d'importanza, sia per ragioni cronologiche, il primo diritto a essere considerato è quello della "privacy in luogo pubblico". Il punto di riferimento nella giurisprudenza della Corte, qui, è dato dal caso che dà il nome a queste pagine, quello di Mr. Katz. Con il caso Katz e il suo test per la privacy in luoghi pubblici, nel 1967, la Corte, rivedendo un proprio precedente del 1928, getta le basi per lo sviluppo della sua stessa giurisprudenza nei decenni a venire.

Quindi (§ 7.3), il riferimento andrà alla "privacy in casa propria", formula che allude all'impatto delle nuove tecnologie sulla privacy con i temi, a noi noti, della nuova sorveglianza. Sebbene la Corte abbia emesso sentenze rivoluzionarie nel settore della privacy domestica, a proposito dell'uso (legittimo) dei metodi contraccettivi (1965), aborto (1973), e omosessualità (2003), il paragrafo si soffermerà in particolar modo sul caso *Kyllo* (2001). Incentrato sulla illegittimità o meno dell'uso dei nuovi dispositivi tecnologici da parte della polizia – nel caso, i sensori termici – *Kyllo* chiarisce come la Corte suprema sviluppi ulteriormente il test introdotto con il caso Katz, onde stabilire quale ragionevole aspettativa di privacy sia d'attendersi per via del progresso tecnologico.

Successivamente (§ 7.4), "a spasso nell'infosfera" espone i problemi cui è andata incontro la Corte con l'ulteriore avanzare della "quarta rivoluzione". La trasformazione radicale che quest'ultima comporta, chiama in causa il modo in cui le regole sociali si possano formare a contatto con il vorticoso progredire della tecnica e se, poi, i giudici di Washington riescano a intercettarle. Precisamente questo è stato il problema discusso nel più recente caso *Jones* del 2012, dove si è avuto un vero e proprio scontro generazionale all'interno della corte, sia pure sotto la forma di opinioni concorrenti (*concurring opinions*), e non dissenzienti (*dissenting opinions*), tra

Antonin Scalia (n. 1936) e Sonia Sotomayor (n. 1954), su come interpretare il caso della sorveglianza continua della polizia tramite GPS.

Infine (§ 7.5), il capitolo tenterà di fare un bilancio, e trarre la prognosi, su "una ragionevole aspettativa di privacy". Alcuni hanno denunciato un vizio logico in tutto il test: affinché la ragionevole aspettativa di privacy da parte di un individuo inneschi il lato sociale di questa stessa aspettativa, è pur sempre necessario che qualcuno corra il rischio di testare per primo la medesima (§ 7.5.1). Altri, ancora, reputano che simili problemi di aspettativa debbano essere disciplinati, e decisi, dal Parlamento piuttosto che dalle Corti (§ 7.5.2). In ogni caso (§ 7.5.3), non dobbiamo perdere di vista il ruolo delle norme sociali nel sistema delle fonti, la cui importanza abbiamo cominciato a vedere in questa introduzione al capitolo. Si tratta in fondo di comprendere le ragioni di Mr. Katz.

## 7.1. *Libertà di parola*

La libertà di espressione è oggi il diritto costituzionale più caro agli americani; per molti versi, il simbolo della stessa libertà in quel paese. Specialmente dopo l'elaborazione giurisprudenziale della Corte suprema presieduta dal giudice Earl Warren (1891-1974), vale a dire tra gli anni 1953 e 1969, il diritto di parola appare come un principio supremo che può essere limitato soltanto da particolari eccezioni, quali la diffamazione o l'oscenità. A differenza della maggior parte degli ordinamenti degli stati democratici occidentali, in cui, spesso, la questione è affrontata come un problema di bilanciamento tra i vari diritti costituzionali in gioco, negli Stati Uniti la libertà di parola è la regola generale che tutela le opinioni razziste del Ku Klux Klan, l'esaltazione della pedo-pornografia in svariati siti web, l'apologia dell'uso delle armi e altro ancora. Il motivo di questa tutela, che può sembrare finanche paradossale a molti fuori dagli Stati Uniti, può essere chiarito con le parole del giudice Thurgood Marshall (1908-1993), nel caso *Police Department of Chicago vs. Mosley* del 1972, per cui "il Primo emendamento significa che il governo non ha alcun potere di limitare la parola a causa del messaggio, le idee, la natura dell'argomento o il suo contenuto. Al fine di permettere il formarsi continuo della nostra cultura e politica, nonché di garantire l'auto-realizzazione di ogni individuo, è garantito al nostro popolo il diritto di esprimere qualsiasi pensiero, libero dalla censura del governo. L'essenza del divieto di censura è il controllo sui contenuti. Qualunque restrizione alla libertà di parola, a causa del suo contenuto, finirebbe per erodere del tutto il pieno impegno nazionale al principio che il dibattito sulle questioni pubbliche sia privo di inibizioni, robusto e aperto a trecentosessanta gradi" (*op. cit.*, 408 U.S. 92).

Su queste basi, possiamo ora restringere lo spettro dell'analisi per considerare, nello specifico, come si rapporti la tutela del Primo emendamento ai temi della privacy. Avendo presente che la tutela tra privati, e cioè tra la loro libertà di parola e la difesa nei confronti di atti diffamatori, diffusione di fatti privati o loro distorsione sotto "falsa luce" è devoluta alla giurisdizione ordinaria nei singoli stati, qui, invece, si tratta di capire come la privacy dei cittadini americani sia protetta nella sfera pubblica per via, appunto, delle garanzie costituzionali del Primo emendamento.

Emblematico, a questo proposito, il caso occorso durante le lotte civili degli anni Cinquanta dello scorso secolo, che vide contrapporsi la *National Association for the Advancement of Colored People* (NAACP) allo stato dell'Alabama [2]. Davanti alla richiesta di quest'ultimo stato di entrare in possesso della lista dei membri dell'associazione in questione – onde fare pressione su di essi per porre termine alle proteste in favore dei diritti dei "*colored*" – la Corte ha riconosciuto la "relazione vitale" esistente tra privacy e libertà d'associazione, per cui "l'inviolabilità della privacy può risultare in molte circostanze indispensabile per preservare la libertà d'associazione, soprattutto quando un gruppo aderisce a opinioni dissidenti" (*op. cit.*, 462). Due anni più tardi, la questione era destinata a ripresentarsi nel caso *Talley vs. California*, in cui la Corte ha dichiarato l'incostituzionalità della legge statale che proibiva la distribuzione di volantini anonimi [3]. La ragione della sentenza era infatti di impedire non solo le sanzioni o ritorsioni da parte delle autorità pubbliche, ma anche da parte di qualunque cittadino che fosse entrato eventualmente in possesso di quelle stesse informazioni. Come ribadito più recentemente in un caso del 1995 [4], "l'interesse che opere anonime possano entrare nel mercato delle idee, senza alcun dubbio ha maggiore importanza di ogni pubblico interesse nel richiedere la comunicazione [dei nomi]. Pertanto, la decisione di un autore di rimanere anonimo, al pari di altre decisioni concernenti omissioni o aggiunte al contenuto della pubblicazione, è un aspetto della libertà di parola protetta dal Primo Emendamento".

Del resto, il principio ha perfino conosciuto una sorta di nuova giovinezza con la rivoluzione informatica. Fermo restando, infatti, l'obiettivo di promuovere l'interesse civico per la partecipazione politica, abbiamo già ripreso e citato parte della sentenza della Corte suprema con cui, nel 1997, era dichiarata la parziale incostituzionalità del *Communications Decency Act*, sulla base della presunzione generale che l'intervento del governo "ostacoli il libero scambio delle idee, piuttosto che incoraggiarlo" (v. § 3.4.1).

Se mai, i problemi che la rivoluzione informatica ha posto sul piano della tutela costituzionale della privacy, riguardano la protezione del quarto, più che del primo, emendamento, ossia "il diritto del popolo di avere sicurezza […] contro ogni irragionevole perquisizione o sequestro".

Il tema riconduce ai nodi emersi con l'uso delle nuove tecnologie ai fini della sicurezza nazionale (§ 6.2.1), in quella che è stata anche definita come società della nuova sorveglianza (§ 6.2.2). Mentre, nel capitolo precedente, l'interesse si è concentrato sulle nuove applicazioni tecnologiche e su come ora il parlamento, ora l'esecutivo, siano intervenuti con leggi, statuti e piani governativi per la sicurezza nazionale, qui, invece, occorre soffermarsi sul sindacato di costituzionalità che si è avuto su tali norme e sulle azioni delle agenzie federali. Tra Quarto emendamento e giurisprudenza della Corte suprema, è questo il tema che ci impegnerà nei prossimi paragrafi.

---

[2] Si tratta del caso *NAACP vs. Alabama*, 357 U.S. 449 (1958).

[3] Cfr. *Talley vs. California*, 362 U.S. 60 (1960).

[4] Il riferimento va a *McIntyre vs. Ohio Board of Elections*, 514 U.S. 334 (1995).

## 7.2. *Privacy nei luoghi pubblici*

Si è detto come la tutela della privacy sia stata originariamente associata al presidio delle quattro mura domestiche come "castello" di ogni uomo (v. § 6.1.3).

Con l'avanzare del progresso tecnologico, nondimeno, già dagli anni venti del secolo scorso era venuta ponendosi la questione se quella protezione, tradizionalmente riferita a perquisizioni o sequestri in casa propria, dovesse estendersi ai luoghi pubblici. Il problema era sorto soprattutto con lo sviluppo della telefonia e la circostanza, illustrata in innumerevoli film dell'epoca, che, per poter parlare al telefono con qualcuno, fosse necessario passare attraverso il filtro dell'operatore telefonico. Inoltre, con il diffondersi delle cabine telefoniche nei luoghi pubblici, nasceva l'ulteriore questione di stabilire se la tradizionale tutela del quarto emendamento valesse anche per le telefonate che uno non faceva più da casa propria ma, appunto, servendosi di tali cabine.

È con la sentenza della Corte suprema nel caso Katz del 1967 che, ribaltando il proprio precedente orientamento, i giudici di Washington hanno ammesso questa nuova forma di tutela: "il Quarto Emendamento protegge il popolo, non i luoghi" (389 U.S. 352).

Oltre l'importanza della decisione in quanto tale, il caso è però particolarmente interessante perché consente d'illustrare un'altra particolarità del sistema americano, vale a dire che con la pubblicazione delle decisioni della corte, veniamo non solo a sapere quale sia stata l'opinione dei singoli giudici; ma, è dato a questi ultimi, ora, di dissentire rispetto alla decisione presa dai colleghi con un'opinione opposta, o alternativa (*dissenting opinion*); ora, di spiegare le proprie ragioni per condividere gli estremi della decisione presa (*concurring opinion*).

Tornando al caso Katz, è da notare infatti che, quando la Corte abbandona il suo precedente in *Olmstead vs. United States*, in realtà, questa decisione del 1928 non era stata presa all'unanimità; bensì, aveva visto l'opposizione strenua di uno dei suoi componenti, a noi, peraltro, ben noto: Louis Brandeis (v. § 6.1). Divenuto dal 1916, fino al '39, giudice della Corte suprema, Brandeis formulerà, nel caso *Olmstead*, una delle più note *dissenting opinions* della storia costituzionale statunitense.

D'altra parte, quando la Corte rivedrà le sue tesi con Katz, questa decisione, negli anni a venire, sarebbe stata ripresa non solo dalla stessa corte, ma anche dal legislatore di Washington, per via soprattutto della *concurring opinion* del giudice Harlan e del test, messo ivi a punto, sulla ragionevole aspettativa di privacy.

Per approfondire i temi della privacy in luogo pubblico, il paragrafo viene di qui suddiviso in quattro parti che hanno per filo conduttore i problemi posti dalla tecnologia del telefono: le ragioni del dissenso di Brandeis in *Olmstead* (§ 7.2.1); le ragioni di Mr. Katz che daranno luogo al capovolgimento giurisprudenziale (§ 7.2.2); il test elaborato da *Justice* Harlan con la sua famosa *concurring opinion* (§ 7.2.3); e le sorti del test negli anni a seguire la sentenza (§ 7.2.4). Ciò condurrà, senza soluzione di continuità, al modo in cui il progresso tecnologico ha modificato anche il tradizionale modo di concepire la tutela della privacy domestica (§ 7.3).

### 7.2.1. *Opinioni dissenzienti*

Nel 1928, la Corte suprema si è pronunciata sulla legittimità costituzionale di condanne penali basate sul materiale probatorio raccolto con intercettazioni prive di mandato, ovvero senza l'autorizzazione dei giudici. Una delle questioni che l'allora recente tecnologia dei telefoni e delle microspie poneva, era, infatti, quella di come interpretare la nozione di "ogni irragionevole perquisizione o sequestro" di cui al Quarto emendamento alla costituzione americana. Fino al caso *Olmstead*, e secondo la secolare tradizione di common law, quelle nozioni erano intese come una "intrusione" o "violazione di domicilio", nel senso in cui l'accezione di *trespass* è correntemente interpretata nell'ambito della responsabilità civile del *tort law*.

Tuttavia, quest'ottica di tipo proprietario, sul modo d'intendere ciò che il Quarto emendamento mira a proteggere da "ogni irragionevole perquisizione", poneva il grosso problema di come inquadrare il caso dell'intercettazione telefonica. In fondo, registrando la voce di un individuo, la polizia certamente s'"intromette" nella vita di questa persona; ma, a che titolo questa intrusione può essere colta come illegittima violazione della proprietà dell'indagato?

Con decisione sofferta, 5 a 4, la Corte giungeva nel 1928 alla conclusione che le intercettazioni telefoniche in realtà avvengono fuori dal domicilio o casa delle persone, per cui "non ricadono sotto la protezione del Quarto Emendamento" (277 U.S. 438). In altri termini, che sono poi quelli che definiranno l'orientamento della corte in materia nei decenni a seguire, l'intercettazione delle conversazioni telefoniche tra i privati, anche senza mandato da parte della polizia, non costituisce né "irragionevole perquisizione" né "sequestro" ai sensi del Quarto emendamento, perché il "sequestro" della voce, da parte delle autorità, non avviene nel "castello di ogni uomo" e, pertanto, non può concepirsi né come "intrusione" né come "violazione di domicilio".

Non era questa, però, l'opinione del giudice Brandeis: come detto, in una delle più famose *dissenting opinions* del diritto costituzionale statunitense, Brandeis stigmatizza la conclusione dei colleghi come un "cattivo incidente d'invasione della privacy" [5].

Ancora una volta, come già quasi quarant'anni prima, ai tempi delle fotografie nello scritto con Warren, *The Right to Privacy* (§§ 6.1 e 6.1.1), Brandeis sottolinea come "il progresso della scienza nel fornire al governo gli strumenti di spionaggio non si fermerà certo all'uso delle intercettazioni telefoniche" e anzi, "strumenti più sottili e di più ampia portata saranno nelle mani del governo". Per cui, prosegue il *Justice*, la Corte suprema avrebbe dovuto estendere la tutela del Quarto emendamento non solo alle conversazioni telefoniche ma, ancor di più, al fine di prevenire "ogni ingiustificabile intrusione del governo nella privacy dell'individuo". L'accento era posto sulla tutela al perseguimento della felicità da parte di ciascuno di noi, come previsto sia dai Padri fondatori (§ 3.1.3.1), sia da Kant, per cui, con le parole di quest'ultimo, si tratta degli "scopi empirici di sorta (i quali tutti sono classificati sotto il nome di felicità)", dei quali Kant ha spiegato le ragioni perché è bene che i governi

[5] Tutte le seguenti citazioni di Brandeis in *Olmstead vs. United States* 277 U.S. 438 (1928).

non se ne interessino (v. § 5.3.3.1). Con le parole di Brandeis in *Olmstead*, i Padri fondatori "hanno conferito, contro il governo, il diritto di essere lasciati indisturbati – il più comprensivo dei diritti e il diritto più apprezzato dagli uomini civili".

Negli anni a venire, l'ombra dell'opinione dissenziente di Brandeis sul verdetto di *Olmstead* si sarebbe fatta sempre più lunga. Nel 1963, in un caso in cui la Corte suprema ammetteva l'uso di registratori nascosti da parte della polizia senza apposito mandato, al fine di raccogliere le prove contro un sospetto, un nuovo giudice, *justice* Brennan (1906-1997), riprendeva le argomentazioni di Brandeis; ma per ricondurle alle garanzie costituzionali del primo, piuttosto che del quarto emendamento, in tema di libertà di parola. Se uno dovesse ammettere la tesi della Corte, spiega Brennan nella sua opinione dissenziente, per cui l'uso di registratori nascosti, senza garanzia giudiziaria, è legittimo, "l'unico modo per tenersi al riparo dal rischio, sarebbe di avere la bocca chiusa in tutte le occasioni". E però, conclude Brennan, "il diritto alla privacy significherebbe poco o nulla se fosse limitato a [tutelare] i pensieri solitari di una persona" (in *Lopez vs. United States*, 373 U.S. 427 (1963)).

Di lì a qualche anno, i tempi sarebbero stati maturi per mutare orientamento. La circostanza sarebbe occorsa, nel 1967, con il caso di un allibratore solito a piazzare scommesse illecite per mezzo di un telefono pubblico. La polizia aveva pensato bene di piazzare nella cabina telefonica una cimice, senza alcun mandato o provvedimento giudiziario, per raccogliere prove a carico del sospetto. Le prove raccolte in questo modo, potevano poi essere legittimamente usate contro l'imputato? Si tratta di "irragionevole perquisizione o sequestro", come tali contrari al Quarto emendamento, o rimane ferma la posizione della Corte in *Olmstead*, per cui, neanche in questo caso, si darebbe alcuna forma di illegittima intrusione, o violazione di domicilio, intesa come *trespass*?

### 7.2.2. *Il caso Katz*

Il mutamento era nell'aria, sebbene né le circostanze né le coincidenze potevano essere previste da qualcuno. In *Berger vs. New York* qualche mese prima, la Corte suprema aveva dichiarato invalida la legge di uno stato dell'Unione, New York, appunto, perché quella legge avrebbe condotto a una "ispezione generalizzata" delle telefonate e, di qui, a una sorveglianza elettronica degli individui incompatibile con le garanzie del Quarto emendamento (388 U.S. 41 (1967)). Più tardi, in quello stesso anno, la Corte si ritrovava a decidere sul ricorso di *certiorari* presentato dagli avvocati Harvey Schneider e Burton Marks, a difesa di Mr. Katz. Secondo un'ulteriore particolarità di quel sistema giuridico, la Corte ha infatti il potere di scegliere i casi da decidere, per cui, dovendo pronunciarsi ora al riguardo del caso di Mr. Katz, al primo voto gli oppositori (i giudici Stewart, Clark, Harlan, White e Black) prevalsero su coloro che volevano invece affrontare il caso: i giudici Brennan, Fortas, Douglas e il presidente della corte *Chief Justice* Warren: 5 a 4.

Il 12 giugno 1967, tuttavia, uno dei cinque giudici che avevano prevalso nel respingere la domanda, *justice* Clark, rassegnava le dimissioni, sostituito da Thurgood Marshall, la cui *opinion* sulla libertà di parola in *Police Department of Chicago vs. Mosley* è stata riportata nel § 7.1. Nondimeno, Marshall si asteneva a sua volta dal caso Katz per motivi di imparzialità, in quanto, nel precedente incarico di avvocato

generale dello stato, era stato proprio Marshall ad aver presentato la memoria del governo degli Stati Uniti contro le tesi di Mr. Katz.

Morale: il 20 ottobre 1967, la Corte, che nel frattempo aveva deciso di discutere finalmente il caso, dopo il dibattimento e l'esposizione a voce delle tesi di ciascuna delle parti, finiva per spaccarsi, secondo la logica degli schieramenti già manifestatasi nel precedente voto sulla richiesta di *certiorari*. 4 a 4. Che fare?

Dal punto di vista giuridico, lo stallo della Corte avrebbe, in sostanza, avallato il comportamento della polizia nel caso dell'allibratore Katz. Ma, dal punto di vista politico, la situazione era particolarmente delicata perché, come spiegherà poi *justice* White nella sua *dissenting opinion*, il Congresso di Washington stava proprio in quei mesi discutendo l'approvazione di una legge in materia di intercettazioni e sorveglianza elettronica. Fare apparire la Corte così drammaticamente spaccata proprio sul punto, rispetto al quale il Congresso avrebbe dovuto avere invece le idee ben chiare, appariva inaccettabile. Due settimane dopo lo stallo, ai primi di novembre, uno dei giudici, *justice* Stewart, cambiava perciò opinione (5 a 3); proponendo però ai colleghi un progetto di decisione che, pur rivedendo il precedente giurisprudenziale di *Olmstead*, consentisse di trovare un compromesso tra i due schieramenti della Corte. Entro il mese, il compromesso venne raggiunto e, 7 a 1, con il solo *justice* White dissenziente, la Corte suprema decise di accogliere e dar ragione alle tesi di Mr. Katz, sulla base del documento messo a punto da *justice* Stewart.

Tuttavia, l'opinione maggioritaria della corte criticava espressamente quello che, a suo dire, era stato il punto di vista sia della difesa, sia dell'accusa, e cioè di concentrarsi sulla natura del luogo, pubblico o privato, in cui si trovava Katz, piuttosto che sulla persona di Katz e, più in particolar modo, sulla tutela della privacy di quell'individuo. Con le parole della Corte, "a causa del modo fuorviante in cui i problemi sono stati formulati, le parti hanno concesso grande significato a caratterizzare la cabina telefonica da cui il richiedente [Katz] ha fatto le sue chiamate. Il richiedente ha strenuamente argomentato che la cabina è 'un'area costituzionalmente protetta'. Il Governo ha parimente sostenuto con vigore che non lo è. Ma questo sforzo di decidere se un''area' specifica, in astratto, sia o meno 'costituzionalmente protetta', distoglie l'attenzione da quale sia il problema da affrontare nel caso. Infatti, il Quarto Emendamento protegge le persone, non i luoghi. Quando una persona espone consapevolmente qualcosa al pubblico, perfino a casa sua o in ufficio, ciò non è soggetto alla protezione del Quarto Emendamento. Ma quando ha cercato di mantenere quel qualcosa privato, anche in un'area accessibile al pubblico, ciò può essere protetto costituzionalmente" (*Katz*, 389 U.S. 351).

Per raggiungere il compromesso tra i giudici, l'opinione maggioritaria preparata da Stewart si premuniva di aggiungere che l'azione di sorveglianza e intercettazione svolta nel caso Katz non è di per sé illegittima: "è chiaro che questa sorveglianza è stata circoscritta così strettamente che un giudice dovutamente autorizzato, e propriamente informato sul bisogno di tale investigazione, specificamente informato sul modo in cui quest'ultima è pianificata, e chiaramente informato sulla precisa intrusione che l'investigazione stessa può comportare, può darne il via libera ai sensi della Costituzione, purché con le cautele del caso e nei limiti specifici dell'investigazione e sequestro richiesto dal Governo" (*op. cit.*, 354). In altri termini, la sorveglianza elettronica degli individui non è di per sé costituzionalmente illegittima e, se solo

avessero avuto l'accortezza di farsi dare un mandato, anche l'attività degli agenti dell'FBI nel registrare le chiamate di Katz sarebbe stata incensurabile.

Tuttavia, nell'abbandonare il precedente di *Olmstead*, la Corte andava incontro a un non piccolo problema: nell'interpretazione proprietaria del quarto emendamento non è infatti così difficile capire cosa sia protetto da "irragionevole perquisizione o sequestro". Secondo i dettami del *trespass* di common law, la protezione è commisurata alla sfera fisica dell'individuo, a partire dalle cose presenti in casa propria, come "castello" a presidio della privacy.

Ma, non appena si allarghi questo punto di vista e, come fa *justice* Stewart, si affermi che la tutela del Quarto emendamento riguarda la privacy degli individui, più che (o oltre a) la tutela delle loro cose, come si fa a stabilire che cos'è un'"irragionevole perquisizione o sequestro" in questo nuovo ambito?

### 7.2.3. *Opinioni concorrenti*

È stato opportunamente segnalato (Winn 2009), come l'opinione concorrente di *justice* Harlan nel caso Katz riprenda l'argomentazione nel dibattimento dell'avvocato di parte, l'allora giovane e inesperto procuratore legale, e ora giudice, Harvey Schneider. Dalla registrazione di quella discussione, ora disponibile su internet, è dato sentire come Schneider concentri l'attenzione della Corte sulla natura della cabina pubblica; ma, non nel senso sottolineato nell'opinione della Corte, e cioè per stabilire se quella cabina pubblica fosse o meno tutelata dal Quarto emendamento. Piuttosto, ciò su cui Schneider invitava i giudici a riflettere è come il suo assistito, Mr. Katz, avesse avuto una legittima aspettativa sul fatto che, entrando nella cabina e cominciando a fare le chiamate, le sue parole non erano destinate a essere di dominio pubblico. In fondo, questa è la legittima aspettativa che chiunque di noi avrebbe in simili circostanze. Il fatto che la Corte abbia poi duramente e, per certi versi, ingiustamente criticato la difesa delle parti e, soprattutto, non abbia preso in considerazione le tesi di Schneider sulla ragionevole aspettativa di privacy, è stato spiegato con la circostanza che l'opinione della Corte e il suo compromesso sarebbero stati formalizzati prima del dibattimento (Winn 2009: 6).

In ogni modo, è significativo che uno dei giudici, John Harlan (1899-1971), abbia prestato attenzione alle argomentazioni di quel giovane avvocato difensore e, perfezionandole, le abbia in séguito presentate in una delle più note opinioni concorrenti della storia costituzionale americana. Con le parole di Harlan, "come afferma l'opinione della Corte, 'il Quarto emendamento protegge la gente, non i luoghi'. La questione, tuttavia, è che tipo di protezione il Quarto emendamento accordi a quella gente. La mia comprensione della regola emersa da decisioni precedenti, è che ci sia un duplice requisito: primo, che una persona abbia mostrato un'attuale (soggettiva) aspettativa di privacy e, secondo, che tale aspettativa sia tale che la società sia pronta a riconoscere come 'ragionevole'. Pertanto, la casa di un uomo è, per lo più, un luogo in cui egli si aspetta di avere privacy, sebbene le cose, attività e dichiarazioni che egli espone alla 'piena vista' degli altri non siano 'protette' perché non c'è stata intenzione di tenerle per sé. D'altra parte, le conversazioni all'aperto non sarebbero protette contro l'essere sentite, per cui l'aspettativa di privacy sarebbe irragionevole in queste circostanze" (389 U.S. 361).

Al precedente criterio fisico e proprietario di *Olmstead* imperniato sull'idea della tutela dal *trespass*, si affianca così un'ulteriore tutela, fondata sul diritto alla privacy, che consiste nel diritto di essere lasciati indisturbati, come voleva Brandeis, anche in luogo pubblico. Questo non significa, va da sé, che la polizia federale o statale non possa svolgere compiti di sorveglianza, pedinamento o intercettazioni; ma, in mancanza delle garanzie che si fondano sull'autorizzazione di un magistrato, l'individuo ha pur sempre il diritto a non essere sottoposto a irragionevoli controlli, tanto in casa propria, come nei luoghi pubblici. Questo diritto, come visto, ha una duplice condizione: la prima, soggettiva, consiste nel fatto che l'individuo, con i propri comportamenti, non si sia volontariamente esposto al pubblico: sebbene le quattro mura di casa siano il "castello" dell'uomo, non ci sarebbe nessuna ragionevole aspettativa per colui il quale, mettendosi a gridare con le finestre spalancate sulla strada, pretendesse, però, che quanto detto in casa propria debba rimanere riservato.

Dopo di che, c'è la condizione oggettiva della tutela, ossia, che la società sia a sua volta pronta a riconoscere tale pretesa soggettiva alla privacy come ragionevole; ciò che, nel caso dell'uso della cabina telefonica da parte di Katz, si deve pur ammettere: ogni americano avrebbe ritenuto irragionevole l'aspettativa di poter trovare cimici della polizia disseminate a ogni cabina telefonica. Per questo verso, il Quarto emendamento rinforza la libertà di parola protetta dal Primo, poiché, per dirla con il giudice Brennan, l'unica maniera per non sottoporsi a questa forma irragionevole di controllo, sarebbe quella di avere sempre la bocca cucita.

Significativamente, fin dall'anno successivo al caso Katz, la Corte suprema si è più volte rifatta a questo suo precedente; ad esempio, il caso viene citato già nel 1968, in *Mancusi vs. De Forte*, a supporto di una nuova opinione maggioritaria della Corte (392 U.S. 368).

Tuttavia, fatto questo per molti versi singolare, già in questo primo rimando della Corte al proprio precedente, non ci si rifà all'opinione maggioritaria elaborata dal giudice Stewart, bensì, avendo come punto di riferimento il test elaborato da *justice* Harlan nella sua opinione concorrente, ossia il test per appurare quando un'aspettativa di privacy è ragionevole o meno e, su queste basi, accordare la tutela del Quarto emendamento.

### 7.2.4. *Il test alla prova*

L'anno dopo il caso Katz, il Congresso di Washington approvava finalmente la riforma della legge federale in materia d'intercettazioni, che i legislatori andavano discutendo fin dal 1967, e cioè ai tempi della spaccatura della Corte suprema sul caso. Con *The Omnibus Crime Control and Safe Street Act*, ossia con le nuove disposizioni del titolo terzo del codice – 18 U.S.C. §§ 2510-20 (1968) – il legislatore ha così tenuto sostanzialmente conto delle indicazioni della Corte, anche al fine di non incorrere in (nuovi) vizi di incostituzionalità, che avevano già colpito l'anno precedente lo statuto di uno stato come in *Berger vs. New York* (§ 7.2.2).

Negli anni a venire, la Corte si sarebbe più volte richiamata al test per dirimere nuovi casi di tutela della privacy sotto la copertura del quarto emendamento: nel 1979, come diremo, in *Smith vs. Maryland*, i giudici di Washington menzionano la "ragionevole aspettativa di privacy" di *justice* Harlan, presentandola come "la nor-

ma di Katz" (442 U.S. 735 e 740); e, ancora nel 1998, in *Minnesota vs. Carter*, il richiamo è testualmente a "*the Katz test* (che è diventato un modo di dire il test enunciato da *Justice* Harlan nella sua opinione concorrente in Katz)" (525 U.S. 83 e 97).

Tuttavia, l'applicazione del test ai nuovi casi di sorveglianza elettronica si è talora rivelata problematica: nel 1971, in *United States vs. White*, la Corte ha ritenuto ammissibili in un procedimento penale le prove tratte dalle conversazioni degli indagati con gli infiltrati della polizia, catturate tramite cimici nascoste. Siccome era pacifico, per i precedenti giurisprudenziali della Corte, che gli agenti di polizia possano trascrivere, registrare o trasmettere elettronicamente una conversazione, senza violare per questo la tutela del Quarto emendamento, il tribunale supremo negava la ragionevole aspettativa di privacy per White. Con le parole dell'opinione maggioritaria dei giudici, "se la legge non accorda alcuna protezione al malfattore che si fida di un complice che è o diventa un agente di polizia, a maggior ragione la legge non lo protegge quando lo stesso agente abbia registrato o trasmesso le conversazioni che poi sono offerte come evidenza, al fine di provare l'accusa" (401 U.S. 752). L'opinione era duramente criticata, nella sua *dissenting opinion*, da *justice* Douglas, per il quale una sorveglianza elettronica sugli individui, senza le dovute garanzie, avrebbe portato a uno stato di polizia, in quanto "ciò che gli antichi conobbero come 'origliare' o 'spiare', ora lo chiamiamo 'sorveglianza elettronica'; ma, considerarle allo stesso modo sarebbe come porre la prima arma da fuoco dell'uomo sullo stesso piano di una bomba atomica" (*United States vs. White*, 401 U.S. 745; la cit. a p. 756).

Più tardi, nel 1979, ci sarebbe stato il famoso caso *Smith vs. Maryland*, sul quale ci siamo soffermati sopra (v. § 6.2.1): in quella occasione, si ricorderà, l'FBI aveva intercettato le chiamate di un sospetto, installando alla centrale telefonica un sistema di registrazione delle sue telefonate, o "pen register", con cui erano state raccolte le prove a carico di Smith. La Corte, come detto, respingeva la tesi che l'imputato potesse aver avuto qualche ragionevole aspettativa di privacy, perché, con la dottrina della "regola della divulgazione a terzi", Smith aveva "assunto il rischio che la compagnia [telefonica] potesse rivelare alla polizia i numeri da lui fatti" (442 U.S. 735, cit. a 743).

Fu una decisione destinata a fare scandalo, tant'è che non solo venne aspramente criticata dalla dottrina (v. Tribe 1988); ma pure dal Congresso, che nel 1986 introdusse importanti modifiche alla legge, approvando un apposito atto, l'*Electronic Communications Privacy Act* o ECPA (1986; 18 U.S.C. §§ 3121-3126); e da altre Corti statali. Nel 1982, ad esempio, la Corte suprema di New Jersey prese espressamente le distanze dai colleghi di Washington, stabilendo che esiste un'aspettativa ragionevole di privacy, anche per ciò che riguarda le chiamate e i tabulati telefonici (*State vs. Hunt* 450 A.2d 952).

In aggiunta ai tormenti della Corte sulle intercettazioni, uno dei problemi giuridici che l'ulteriore progresso tecnologico avrebbe dovuto proporre alla Corte suprema, di lì a poco, riguarda l'ambito forse più naturale per l'applicazione del test, vale a dire la ragionevole aspettativa di privacy in casa propria e a contatto, tuttavia, con nuovi prodotti e ricavati tecnologici che danno un senso nuovo al controllo sulle abitazioni degli individui (§ 6.2.3). Mentre, nel caso delle intercettazioni, da *Olmstead* (1928) a Katz (1967), e fino ai giorni nostri, il problema della tutela accordata

dal Quarto emendamento è ruotato attorno all'uso dei telefoni, a presidio del diritto individuale alla privacy anche in luogo pubblico, a partire dalla seconda metà degli anni ottanta un numero crescente di casi si è incentrato piuttosto sull'uso di nuovi strumenti come fotocamere per aerei, già di uso comune all'inizio degli ottanta, che danno vita a un modo nuovo di visionare quelle case, o gli impianti industriali; secondo una tendenza che avrebbe poi condotto, negli anni 2000, alla tecnologia di Google Maps e, all'inizio della seconda decade, dei droni civili.

Questa nuova generazione di casi discussi all'insegna del Quarto emendamento può essere fatta risalire al 1986, l'anno dell'approvazione dell'ECPA, con la decisione della Corte suprema in *Dow Chemical Co. vs. United States*. Il nocciolo della questione può essere racchiuso nella seguente domanda: qual è la ragionevole aspettativa di privacy che un individuo può avere nell'era dell'aeronautica civile, quando piccoli aerei possono essere usati da privati per sorvolare le città, o altri luoghi, e poi magari fare qualche scatto fotografico?

Fino a *Dow Chemical*, la dottrina consolidata asseriva che non vi fosse ragionevole aspettativa di privacy nei "luoghi aperti" (*open fields*); anche quando l'individuo abbia cercato di proteggersi dallo sguardo pubblico. In altri termini, non possiamo pensare di andare nudi in un parco pubblico, o anche nel giardino di casa propria, adiacente a una strada affollata, e poi pretendere che tutto ciò passi inosservato.

Ma quale, invece, la ragionevole aspettativa di privacy che uno può pretendere, quando si comincia a riprendere da un aereo, casa mia, tramite foto e, più tardi, video? Come devo regolarmi quest'estate, nella piscina del giardino di casa, quando vedrò passare non troppo distante un piccolo drone?

Con le parole della Corte suprema, "il fare fotografie di un impianto industriale da uno spazio aereo consentito alla navigazione, non è un'intrusione (*search*) proibita dal Quarto emendamento" (476 U.S. 239). Infatti, "il mero fatto che la visione umana sia in qualche modo aumentata, almeno fino al punto considerato in questo caso, non solleva particolari problemi costituzionali" (*ibidem*). Sebbene la Corte ammetta che "sorvegliare la proprietà privata con un sistema di sorveglianza altamente sofisticato e non disponibile in genere al pubblico, come la tecnologia satellitare, possa essere costituzionalmente illegittimo in mancanza di un mandato" (p. 237), ciò non sarebbe occorso nel caso oggetto di decisione. In *Dow Chemical*, infatti, si trattava pur sempre di fotografie fatte da un aereo con macchine acquistabili in qualsiasi supermercato o grande magazzino, per cui, secondo l'opinione maggioritaria della corte, dovremmo pensare che le foto prese in questo caso dall'aereo siano legittime e costituzionalmente protette, in quanto ciò che è stato immortalato del complesso industriale è in uno "spazio aperto" (*open field*).

Nonostante l'approccio della Corte possa essere ritenuto ragionevole in molte circostanze, rimane tuttavia aperto il problema posto dall'ulteriore, imperioso sviluppo della tecnologia; per cui, per dirla con le parole critiche di *justice* Burger in *Dow Chemical*, come dovremmo regolarci nel caso di ulteriori ricavati tecnologici, capaci "di penetrare pareti o finestre, così da udire e registrare discussioni confidenziali su formule chimiche o altri segreti industriali"? (476 U.S. 239).

Tre lustri dopo, lo scenario visionato dal giudice Burger si sarebbe materializzato con il caso di un ragazzo che aveva fatto crescere, all'interno della propria abitazione, piante di marijuana con l'uso di lampade ad alto voltaggio. La polizia aveva pen-

sato bene di piazzare un congegno ad immagini termiche nei pressi della casa, senza però avere il mandato per verificare (e provare) la condotta penalmente rilevante dell'indagato. Solo dopo aver raccolto sufficiente evidenza probatoria, l'FBI si era infatti rivolto al giudice per avere il mandato e, con detta autorizzazione, presentarsi a casa del malvivente, perquisirla e sequestrargli il corpo del reato.

Davanti all'obiezione che simile tecnica costituisse in effetti una violazione della privacy, la polizia ha controbattuto che il calore emesso dalle lampade ad alto voltaggio, in realtà, era venuto a diffondersi in luogo pubblico, dove gli ufficiali di polizia avevano potuto acquisire legittimamente le prove con l'impiego di un computer termico digitale.

Si tratta forse di una "perquisizione irragionevole" ai sensi del Quarto emendamento? Nel coltivare piante di marijuana in casa propria, c'è forse una ragionevole aspettativa di privacy?

## 7.3. *Privacy in casa propria*

La tutela della privacy degli individui in casa propria è, per molti versi, l'ambito più naturale in cui possiamo ritrovare la tutela del quarto emendamento: non è un caso che la Corte suprema se ne sia occupata in più occasioni, specie a partire dagli anni sessanta dello scorso secolo, con alcune pronunce a dir poco rivoluzionarie, sia sul piano del diritto, sia sul piano dei costumi sociali.

Tra i casi maggiormente eclatanti, va certamente segnalato per primo quello di *Griswold vs. Connecticut* del 1965 (381 U.S. 479); due anni, dunque, prima del caso Katz.

In quella occasione, la questione ruotava attorno alla messa al bando dell'uso di contraccettivi e, in particolare, dei profilattici da parte (beninteso) delle coppie sposate: la prima tecnica per la contraccezione intrauterina era stata nel frattempo messa a punto da Jack Lippes nel 1961. È interessante segnalare come nel caso di specie, la Corte, per prima cosa, sia partita dall'ammissione che non è dato trovare nel testo della Costituzione americana, un esplicito richiamo alla tutela della privacy. È un problema, del resto, già emerso nel corso delle pagine precedenti (§ 4.1.2), con i dubbi della Cassazione e la decisione della Consulta nel 1973, a proposito della tutela della riservatezza in Italia. Nel caso *Griswold vs. Connecticut*, la strategia della Corte suprema per affrontare il problema, è stata quella d'illustrare la forza espansiva dei principi giuridici, al pari di quanto svolto egregiamente da Warren e Brandeis in *The Right to Privacy*, richiamandosi all'"eterna giovinezza del common law" (§ 6.1.1), sulla base di un'allegoria. La Corte paragona i diritti tutelati dalla lettera degli emendamenti alla costituzione americana con la luce prodotta dalle stelle del firmamento: nel mettere in chiaro certi diritti, come la libertà di parola, ogni emendamento crea al contempo una zona di penombra, entro la quale è tuttavia possibile ricavare la presenza di altri diritti egualmente protetti dalla costituzione, come, appunto, il diritto alla privacy.

A ben vedere, l'unica forma per dar corso alla legge, secondo i consueti modi della tecnica "se A, allora B", in casi come quelli che oppose i coniugi Griswold allo stato del Connecticut, sarebbe stato di cogliere i Griswold nell'atto coniugale, ma-

gari nel talamo della propria casa ("A"), per provvedere a eseguire la penalità della legge prevista dallo stato dell'Unione ("B"). Il 7 giugno 1965, con verdetto 7 a 2, la corte presieduta da Earl Warren, nell'affrontare irreversibilmente un bivio nella storia americana – la questione, in effetti, da allora non si è più riproposta – liquida per sempre il dubbio con una battuta: "dovremmo forse consentire che la polizia investighi nei sacri precinti della camera da letto coniugale, alla ricerca dei segni rivelatori dell'uso di contraccettivi? La stessa idea ripugna alle nozioni di privacy che circondano la relazione matrimoniale" (381 U.S. 486). Si tratta dello stesso principio che, sia pure a maggior fatica, avrebbe fatto strada nella giurisprudenza della corte anche in materia di relazioni tra omosessuali.

Significativamente, nel 1986, in *Bowers vs. Hardwick*, la Corte ha in un primo momento sostenuto la legittimità della normativa dello stato federato di perseguire penalmente i rapporti omosessuali – in specie, il reato di sodomia – in quanto, sia pure trattandosi di rapporti consenzienti tra maggiorenni, essi non avrebbero avuto diritto di intrattenere simili rapporti in nome della privacy, dato che tale condotta sarebbe andata contro una lunga tradizione culturale e giuridica degli Stati Uniti d'America (478 U.S. 186). Qualche anno dopo, nel 2003, in *Lawrence vs. Texas*, la Corte ha però ribaltato il proprio orientamento poiché, secondo l'opinione maggioritaria del giudice Kennedy, "quando la sessualità si manifesta palesemente nell'intimo comportamento con un'altra persona, tale comportamento non è che un elemento nel legame personale" che è costituzionalmente protetto (539 U.S. 567). In fondo, non si tratta poi di una tecnica ermeneutica sconosciuta in Italia, se si pensa ai giudizi di costituzionalità sulle norme del codice penale che, all'articolo 559, prevedevano originariamente un diverso trattamento nel caso d'adulterio da parte dell'uomo, come tale perseguibile solo a querela di parte, e l'adulterio da parte della donna perseguibile d'ufficio. Se, nel 1961, la Consulta di Roma ha dichiarato la legittimità della disparità di trattamento, nel 1968 essa ha cambiato posizione "tenuto conto del mutamento della coscienza civile" del popolo italiano [6].

Più intricato, e altamente controverso, è stato il caso dell'aborto: seppure ciò possa sembrare bizzarro al giurista europeo, sempre in nome della privacy, la Corte ha dichiarato l'illegittimità costituzionale delle leggi di quasi tutti gli stati dell'Unione che criminalizzavano l'aborto: "il diritto di privacy è sufficientemente esteso da comprendere la decisione della donna se porre fine o meno alla gravidanza" (*Roe vs. Wade* del 1973, in 410 U.S. 153). Ciò ha condotto la Corte a rivedere spesso, sia pure parzialmente, la propria posizione originaria: se dal primo caso *Griswold* a *Roe vs. Wade* si abbandona il tradizionale approccio alla privacy in chiave maritale, con il successivo caso *Planned Parenthood of Central Missouri vs. Danforth* del 1976, non era più richiesto il consenso del padre, o del marito, ai fini dell'aborto, e così via.

Ma, senza approfondire anche questo ambito della giurisprudenza costituzionale della Corte, ancora in pieno svolgimento, la ragione di questa tutela della privacy sotto l'egida del Quarto emendamento è chiara: tra individuo e stato, c'è una "zona franca" per la quale è proibito l'intervento del governo federale, o degli stati federa-

[6] Le sentenze della Corte costituzionale italiana sono, rispettivamente, la n. 64 del 28 novembre 1962 e le nn. 126 e 127 del 19 novembre 1968, in rapporto agli art. 3 e 29 della Costituzione.

ti, negli affari privati degli individui. Secondo gli intendimenti filosofici di Kant, ma anche con il disegno politico-istituzionale dei Padri fondatori, è bene che le autorità pubbliche non si intromettano negli "scopi empirici di sorta" e, cioè, su come gli individui intendano perseguire la loro felicità (§ 7.2.1). Fermo restando l'ulteriore principio (kantiano) di non esercitare la propria libertà per nuocere agli altri, la protezione della casa, "castello" di ogni individuo, ha di qui rappresentato, a partire dagli anni sessanta e settanta del secolo scorso, un perno indiscusso delle libertà civili protette dalla costituzione americana, dato che essa è la forma in cui si è cominciato a garantire la libertà di scelta e lo stile di vita di ogni persona.

In parallelo ai casi sui costumi e la moralità sessuale, abbiamo però visto anche l'altro filone di tutela del Quarto emendamento, relativo alla sorveglianza elettronica e le intercettazioni telefoniche: da *Olmstead* (1928) a *Katz* (1967).

L'aspettativa di privacy che possiamo attenderci in questo caso, non riguarda evidentemente le proprie preferenze sessuali o i problemi familiari, stando in casa propria. Inoltre, non si tratta nemmeno della tormentata questione sul diritto che si ha in nome della privacy, quando si fa una telefonata.

Piuttosto, il problema riguarda l'uso di congegni tecnologici che consentono un modo nuovo di visionare e capire, almeno in parte, cosa stia succedendo in una casa: se, come abbiamo cominciato a vedere nel paragrafo scorso, a proposito di *Dow Chemical*, la tecnologia discussa erano gli aerei e le macchine fotografiche, dovremo prendere in considerazione a continuazione, nel prossimo paragrafo, un nuovo tipo di tecnologia: i sensori biotermici computerizzati.

Questa tecnologia ripropone il problema di come interpretare il divieto di "ogni irragionevole perquisizione o sequestro" stabilito dal Quarto emendamento, quando uno scopre, come occorso a Kyllo, di essere sorvegliato senza mandato dalla polizia: la (soggettiva) ragionevole aspettativa di privacy da parte di Kyllo in casa propria. C'è una (oggettiva) ragionevole aspettativa di privacy in questo caso?

La polizia si era infatti appostata sul bordo della strada adiacente all'abitazione di Kyllo, piazzando un sensore termico computerizzato di ultima generazione, con cui poteva tecnicamente registrare e visualizzare i gradi e fonti di calore della casa, e capire molte delle cose che stavano capitando in quella abitazione. Cambia le cose che Kyllo stesse coltivando, illecitamente, marijuana?

### 7.3.1. *Il cas*o *Kyllo*

La risposta della Corte, l'11 giugno 2001, 5 a 4, è stata che, in omaggio al test sulla aspettativa di privacy elaborato da *justice* Harlan nel caso Katz, Kyllo aveva ragione e, quindi, la sorveglianza della polizia con sensori termici, senza mandato, doveva ritenersi costituzionalmente illegittima (533 U.S. 27). Con le parole dell'estensore della decisione, Antonin Scalia, "benché possa essere difficile precisare il test di Katz in certi casi, nel caso dell'intrusione nell'interno di una casa – la prototipica e, di qui, comunemente più controversa area di tutela della privacy – c'è già un criterio che affonda le sue radici nel common law, per cui un minimo di aspettativa di privacy esiste e ciò è riconosciuto essere ragionevole. Indebolire la protezione di questa minima aspettativa vorrebbe dire permettere alla tecnologia di sorveglianza [*police technology*] di erodere la privacy garantita dal Quarto emendamento" (*op. cit.*, 33).

Non ha per ciò rilevanza che la polizia si sia, per così dire, limitata all'uso di un computer che non avrebbe mostrato né le attività in corso all'interno della casa dell'indagato, né avrebbe registrato le conversazioni o svelato i dettagli della vita intima delle persone. Inoltre, con buona pace delle tesi sostenute dalle corti di merito, che avevano condannato Kyllo, non era nemmeno rilevante per il caso di specie, far notare che la polizia si era limitata a prender nota del calore che emanava dalla casa, senza entrare nel domicilio del sospetto, ma limitandosi a stare in luogo pubblico. In realtà, per riprendere Scalia, "questa interpretazione meccanica del Quarto emendamento è stata respinta in *Katz*, dove lo strumento per l'intercettazione ambientale selezionava solo alcune onde che raggiungevano l'esterno della cabina telefonica cui quello strumento era attaccato. Capovolgere l'approccio lascerebbe il proprietario di una casa alla mercé del progresso tecnologico – includendo la tecnologia a immagini che potrebbe discernere tutta l'attività umana in un'abitazione" (*op. cit.*, 35).

Su queste basi, Kyllo aveva per ciò ragione nel sostenere di aver avuto una ragionevole aspettativa di privacy, violata dall'FBI nel metterlo sotto sorveglianza senza mandato, perché "noi crediamo che ottenere con tecnologie d'accrescimento sensorio ogni informazione riguardante l'interno dell'abitazione che non possa altrimenti essere ottenuto senza intrusione fisica in un'area costituzionalmente protetta […] costituisce una perquisizione – almeno quando (come nel presente caso) la tecnologia in questione non sia d'uso pubblico generale" (*op. cit.*, 34).

Tuttavia, è proprio questa la ragione per cui la Corte si è spaccata nel decidere il caso, con la scelta dei giudici Rehnqvist, O'Connor e Kennedy di unirsi al collega *justice* Stevens nell'esprimere un'opinione dissenziente.

A ben vedere, nell'assolvere Kyllo, l'opinione maggioritaria della Corte ha trovato nell'uso di una tecnologia non di uso comune presso il grande pubblico, da parte dell'FBI, il motivo per cui la sua attività di sorveglianza doveva ritenersi illegittima: si tratta di un orientamento giurisprudenziale che abbiamo già visto con *Dow Chemical* nel precedente paragrafo.

Ma, cosa avrebbe mai dovuto dichiarare allora la Corte, qualora la tecnologia messa in campo dall'FBI nel caso Kyllo fosse stata d'uso comune?

Nell'esaminare a suo tempo il caso (Pagallo 2008: 75), notavo la pericolosità dell'inciso "almeno quando" nell'opinione maggioritaria della corte. La vorticosa accelerazione del progresso tecnologico finisce infatti, puntualmente, per rendere in pochi mesi d'uso comune anche i più sofisticati congegni d'ultima generazione. Nel commento al caso Kyllo, facevo riferimento alla produzione e vendita dei visori notturni, già di moda tra il grande pubblico a metà degli anni 2000. Dovremmo di qui aspettarci che la polizia pattugli, senza mandato, le strade della città e osservi nell'oscurità, grazie ai visori, cosa succede dentro le mura domestiche? Tanto più le tecnologie della sorveglianza, come ai giorni nostri i droni, entreranno a disposizione del grande pubblico, tanto più dovremo attenderci che la polizia usi tutti questi strumenti di routine, senza mandato, ai fini della sorveglianza, prevenzione o controllo?

In fondo, è questa la maggiore preoccupazione espressa da *justice* Stevens nella opinione dissenziente a Kyllo, quando afferma che l'"almeno quando" di Scalia "è in qualche modo perverso dato che sembra altamente probabile che il pericolo per la privacy aumenterà, piuttosto che diminuire, nella misura in cui l'uso di congegni

intrusivi diventerà sempre più facilmente disponibile". La ragionevolezza della critica dipende dal fatto che, contrariamente allo spirito del test messo a punto da *justice* Harlan, l'accento di Scalia cade di più su come si diffonda l'uso degli strumenti tecnologici nell'insieme della società, che sui vincoli normativi che dovrebbero disciplinarne l'uso. Quando abbiamo visto Brandeis inventare la formula del "diritto alla privacy" nel 1890, e poi difenderla nei fatti, come giudice della Suprema, con una memorabile *dissenting opinion* nel 1928, l'idea che egli proponeva della privacy come diritto di essere lasciati indisturbati, a casa propria, come anche in luogo pubblico, era pur sempre volta a limitare un certo uso della tecnologia, piuttosto che assistere, passivi, al suo travolgente progresso.

Durante la vita di Brandeis, l'evoluzione tecnologica avrebbe condotto dai problemi giuridici dell'impatto delle prime foto istantanee (1890), all'uso di massa dei telefoni (1928). Più tardi, attraverso le sentenze della Corte suprema, siamo passati dalle foto aeree di *Dow Chemical* nel 1986, ai sensori termici di Kyllo nel 2001.

È giunto ora il turno per l'esame della tecnologia GPS.

## 7.4. *A spasso nell'infosfera: privacy digitale*

Nel capitolo precedente, abbiamo visto il modo in cui la tecnologia incida sulla rappresentazione del concetto di privacy (figura 18), con gli esempi delle fotografie (§ 6.1.1), delle banche dati (§ 6.1.2), e del Web 2.0 (§ 6.1.3).

In questo capitolo, abbiamo illustrato questo riposizionamento tecnologico con i problemi relativi alla tutela del Quarto emendamento nella giurisprudenza della Corte suprema, in relazione alla tecnologia del telefono (§ 7.2.1), alle cabine telefoniche (§ 7.2.2), le camere fotografiche per aerei (§ 7.2.4), e i sensori termici (§ 7.3.1). Dal punto di vista della ragionevole aspettativa di privacy, siamo passati dall'aspettativa in luogo pubblico all'aspettativa di privacy domestica a contatto con i nuovi strumenti e sistemi della sorveglianza. È stato il caso delle tecnologie d'accrescimento sensorio di Kyllo e dei satelliti cui fa cenno la Corte nel caso *Dow Chemical*.

L'ulteriore progresso tecnologico, tuttavia, ha finito per sollevare un terzo ordine di questioni, relativamente alla privacy che uno aspetta di avere nella propria vita, nonostante abbia in tasca un telefono cellulare (destinato a diventare, verso la metà del primo decennio del nuovo secolo, uno *smartphone* o *app-phone*). Nel 2014, la potenza di calcolo di questi apparecchi non solo è diventata mille volte superiore al processore più veloce che si potesse mai avere, nel 1967, ai tempi di Katz; ma, al pari dei vostri tablet, computer e autoveicoli, questi nuovi telefoni dispongono, tra le altre cose, della tecnologia GPS, o sistemi di geo-posizionamento, per sapere dove sia un negozio di scarpe o di sci nelle vicinanze, collocare la vostra macchina in una mappa stradale in tempo reale e dove si trovino i vostri figli (o genitori) in questo momento. Accanto agli usi positivi che si possono fare del GPS e dei suoi derivati, come i servizi che ruotano attorno ai vostri (o altrui) spostamenti, c'è però, naturalmente, il rovescio della medaglia; ossia che il GPS sia utilizzato dalle forze dell'ordine per monitorare i movimenti di un indagato o di un semplice sospetto.

Come detto (§ 6.2.2), questo "doppio uso" della tecnica non significa che essa sia neutra, semplice strumento ai fini più vari. Piuttosto, questo doppio uso sta a ri-

cordare come la tecnologia riplasmi il senso fin qui dato a nozioni chiave per interpretare la tutela del Quarto emendamento, come l'atto stesso del "sorvegliare". Attraverso l'uso del GPS, in fondo, è possibile fare con minimo sforzo ciò che, ai tempi di Katz e fino a un decennio fa, avrebbe richiesto il coordinamento di una squadra di agenti pedinatori, con riprese video e l'uso di aerei o elicotteri, per seguire e tenere sotto controllo i movimenti di una persona, ventiquattro ore su ventiquattro.

Per quanto concerne il rapporto tra i privati, abbiamo visto sin dalla fine dello scorso capitolo (§ 6.3.3), che negli USA esso è lasciato per lo più all'autonomia delle parti, sulla base di contratti e termini di servizio: nel caso dei servizi GPS applicati alla telefonia mobile, ciò significa che le grandi compagnie del settore, come Verizon o AT&T, s'impegnano a rispettare le regole che esse stesse si sono date tramite codici di auto-disciplina.

Ma, che dire quando è il governo (la polizia federale) a far uso della tecnologia del GPS ai fini di sorveglianza? Che ragionevole aspettativa di privacy può uno attendersi in America? Il fatto che questa tecnologia sia oramai d'uso comune, a differenza dei sensori termici di Kyllo, ne liberalizza l'uso nelle operazioni di controllo da parte delle forze dell'ordine?

Questo è l'insieme di domande discusse davanti alla Corte suprema l'8 novembre 2011, nel caso consegnato poi alla storia come caso Jones.

In *United States vs. Jones* (565 U.S. _), infatti, gli agenti federali avevano ottenuto dal giudice un mandato per posizionare nella macchina della moglie di Mr. Jones, un piccolo rintracciatore a GPS, con cui seguire gli spostamenti dell'indagato (che, per la cronaca, come ci informa la stessa Corte nella sua opinione sul caso, commerciava, tra casa e night club, qualcosa come 97 chili di cocaina e uno di cocaina base).

Tuttavia, il giudice che aveva dato l'autorizzazione a seguire Jones con il GPS, posto sotto la sua Jeep, aveva ristretto il mandato della polizia federale a 10 giorni e nel distretto della Columbia: invece, gli agenti dell'FBI pensarono bene di piazzare il congegno sotto la Jeep di Jones all'undicesimo giorno e, peraltro, nello stato del Maryland.

Per altri 28 giorni gli agenti federali "pedinarono" Jones – e, cioè, seguirono in diretta tutti i suoi spostamenti in macchina per quasi un mese – fino a raccogliere le prove per l'accusa di cospirazione nel traffico di droga, per cui, tra le altre cose, Jones finiva per essere condannato all'ergastolo. Secondo il verdetto della Corte distrettuale, in primo grado, era vero che, per ragioni di privacy, si dovevano distruggere i dati raccolti dall'FBI con la tecnologia del GPS, quando la macchina dei Jones era parcheggiata nei pressi della loro casa. Ma, non così, invece, si doveva procedere per i dati ottenuti con gli spostamenti di Jones da un luogo all'altro. Infatti, ragionava la Corte distrettuale, Jones non avrebbe avuto una ragionevole aspettativa di privacy nel viaggiare con la sua macchina, tra casa, night club e amici, per le strade pubbliche.

Sebbene il verdetto sia stato in séguito cassato dalla Corte del circuito distrettuale di Washington, per la sua rilevanza il caso veniva nondimeno ammesso all'ulteriore discussione davanti alla Corte suprema: il 23 gennaio 2012, quest'ultima perveniva alla sua decisione.

Significativamente nessun giudice ha manifesto il proprio dissenso all'opinione stesa da Antonin Scalia, benché tanto *justice* Sonia Sotomayor, quanto il giudice Ali-

to con i colleghi Ginsburg, Breyer e Kagan, abbiano presentato un'opinione concorrente (nel caso di Sotomayor), e un'opinione concorrente nella formula del giudizio (Alito con gli altri).

Partiamo dall'opinione di Scalia.

### 7.4.1. *Il caso Jones*

*Justice* Scalia è noto per il suo impegno ermeneutico teso a interpretare la lettera della Costituzione nordamericana come avrebbero fatto i Padri fondatori e secondo i precedenti della gloriosa tradizione del common law. Non sorprenderà, pertanto, che nel caso Jones, Scalia dia ragione a quest'ultimo, ma non rifacendosi ai più recenti precedenti della corte nel caso Katz (1967), o nel caso Kyllo (2001). Scalia inquadra infatti la fattispecie sulla base di un vecchio precedente del 1765 che, a suo dire, era indubbiamente familiare a ogni statista americano al momento di dover varare la costituzione e, più tardi, integrarla con i divieti posti, tra gli altri, dal Quarto emendamento. Sulla scorta di *Entwick vs. Carrington* (95 Eng. Rep. 807 (C. P. 1765)), Scalia censura il comportamento degli agenti federali come intrusione illegittima o *trespass*, dato che era stato necessario agli agenti di intromettersi fisicamente nella vita di Jones, allorquando posizionavano il congegno GPS sotto la macchina della moglie, il giorno dopo che erano scaduti i termini fissati dal giudice che aveva autorizzato l'operazione.

Scalia ricorda come, rispetto alla tradizionale forma di interpretare le nozioni di "ogni irragionevole perquisizione o sequestro" come *trespass*, sia subentrata nel frattempo l'indubbia novità del caso Katz, per cui la tutela del Quarto emendamento va rivolta al diritto alla privacy degli individui, piuttosto che alla stretta protezione della loro proprietà privata. Così, afferma Scalia nel caso Jones, "il Governo argomenta come il test di Harlan mostri che nessuna intrusione è avvenuta qui, perché Jones non aveva alcuna 'ragionevole aspettativa di privacy' sia nell'area della Jeep in cui erano intervenuti gli agenti federali, sia negli spostamenti della Jeep lungo le strade pubbliche, che sono visibili a tutti. Tuttavia, non dobbiamo seguire il ragionamento del Governo, perché i diritti di Jones protetti dal Quarto emendamento, non dipendono dalla dottrina Katz, né ricadono sotto di essa" (565 U.S. _, p. 5).

Infatti, prosegue Scalia, il diritto alla privacy protetto a partire dal caso Katz, ha indubbiamente ampliato la tutela garantita in nome del Quarto emendamento; ma, ciò non significa che la vecchia protezione contro le violazioni di domicilio o sequestri sia venuta meno: "il test di Katz sulla ragionevole aspettativa di privacy è stato aggiunto, e non si è sostituito, al test dell'intrusione messo a punto dal common law" (*op. cit.*, 8). A volte, può essere necessario ricorrere al test di Harlan, come nel caso Kyllo; ma, quando si tratta di un caso d'intromissione fisica illegittima, come nel caso Jones, il test del *trespass* è sufficiente per risolvere il caso.

Nella seconda parte della sua opinione, Scalia passa poi in rassegna le obiezioni mosse dai colleghi, che avremo modo di esaminare in dettaglio nel paragrafo seguente (v. sotto § 7.4.1.1). In particolare, a chi, come al giudice Alito, sembra bizzarro risolvere un caso sull'uso del GPS nel 2012 con un precedente del diciottesimo secolo, per cui il caso Jones avrebbe richiesto "esclusivamente il test sulla ragionevole aspettativa di privacy in Katz, anche quando ciò elimini diritti previamente

esistenti" (*op. cit.*, 11), Scalia ammette che l'uso dei nuovi ricavati tecnologici solleva in effetti una serie inedita di questioni rispetto al canonico modo di pedinare e sorvegliare le persone: "può essere che ottenere lo stesso scopo con mezzi elettronici, senza intrusione fisica, sia una invasione costituzionalmente illegittima della privacy; ma, il presente caso non richiede che si dia una risposta alla questione. Peraltro, una volta che si dia una risposta affermativa alla domanda, ciò conduce senza bisogno a una serie di spinosissimi problemi addizionali" (*ibidem*); come, ad esempio, stabilire per quali tipi di delitti la sorveglianza continua con GPS possa considerarsi legittima, o per quanto tempo. "È possibile che si debba avere a che fare con questi 'problemi esasperanti' in qualche caso futuro, in cui la classica intrusione da *trespass* non è in gioco e si debba ricorrere all'analisi di Katz; ma non c'è ragione di spingersi qui oltre, per risolvere il caso" (*op. cit.*, 12).

Quest'ultima è proprio la ragione per cui non ci sono state opinioni dissenzienti: si può dare ragione a Jones sulla base del vecchio test di common law sul *trespass* e non dividersi platealmente sul diverso modo in cui si ritiene che si debbano affrontare i nodi della società della nuova sorveglianza, alla luce del test sulla ragionevole aspettativa di privacy.

Le ragioni del dissenso, nondimeno, sono emerse tutte: esse, come diremo a continuazione, hanno preso le forme di due opinioni concorrenti.

#### 7.4.1.1. *Il dissenso nelle opinioni concorrenti*

La ragione del contrasto tra l'opinione maggioritaria a cura di Antonin Scalia e l'opinione concorrente nel giudizio di Alito, con Ginsburg, Breyer e Kagan a suo fianco, ruota innanzitutto attorno all'uso da parte di Scalia, del vecchio test proprietario sul *trespass* messo a punto dalla tradizione di common law. Per un verso, Alito nutre dubbi sul fatto che il congegno a GPS collocato dalla polizia sotto la macchina di Jones costituisca di per sé un'"intrusione": nel caso in cui, infatti, quel "congegno non avesse funzionato, o gli agenti non lo avessero attivato, non si sarebbe ottenuta alcuna informazione" (565 U.S. _, p. 2). D'altro canto, prosegue Alito, è "quasi impossibile pensare che certe situazioni del XIX secolo siano analoghe a quanto successo in questo caso" (*op. cit.*, 3). A riprova, basterebbe soffermarsi sul precedente invocato da Scalia, per cui bisognerebbe immaginare il caso di un poliziotto che si intrufoli dentro la carrozza (a cavalli) di qualcuno, rimanendovi il tempo sufficiente per monitorare e seguire i movimenti del proprietario della carrozza: "la Corte suggerisce che qualcosa di simile debba essere successo nel 1791, ma questo avrebbe richiesto una carrozza gigante, oppure un poliziotto molto piccolo, o entrambi – per non menzionare un poliziotto con incredibile fortitudine e pazienza" (*ibidem*).

In realtà, la Corte ha smesso da tempo di essere ossessionata dalla visione proprietaria e fisica dell'intrusione sanzionabile ai sensi del Quarto emendamento. Muovendo dalle critiche di Brandeis nella sua opinione dissenziente in *Olmstead* (1928), fino alla nuova forma di tutela fondata sulla privacy, e non sulla proprietà privata, di Katz (1967), e con Kyllo (2001), bisogna infatti ammettere che "un'intrusione non è né condizione necessaria, né sufficiente, per incorrere in una violazione costituzionale" (*op. cit.*, 6). Di qui, per decidere se l'aspettativa di privacy, nel caso

Jones, sia ragionevole o meno, non si tratta di appurare le questioni di intrusione, o contatto fisico, tra la macchina di proprietà dei Jones e gli agenti della polizia nell'atto di piazzare il congegno di sorveglianza tramite GPS. Piuttosto, il caso invita a riflettere sulle nuove forme di sorveglianza elettronica, che nulla hanno a che fare con un contatto fisico – come i dati che mandiamo attraverso i servizi GPS dagli *smartphone* – e che rendono del tutto insufficiente il test proprietario messo a punto da Scalia. "Il fatto che la Corte fondi la sua tesi sul diritto di *trespass* porrà problemi particolarmente esasperanti nei casi riguardanti una sorveglianza condotta attraverso un contatto elettronico, come tale opposto a quello fisico, con ciò che è da tracciare" (*op. cit.*, 9).

Alito non si nasconde, tuttavia, i nuovi problemi che tale sorveglianza elettronica pone nei confronti del test sulla ragionevole aspettativa di privacy perfezionato dalla Corte a partire dal caso Katz. Innanzitutto, non senza malizia, egli nota come il test "implichi un grado di circolarità […] e i giudici sono inclini a confondere le loro stesse aspettative di privacy con quelle dell'ipotetica persona ragionevole a cui guarda il test di Katz" (*op. cit.*, 10, dove si cita il precedente *Minnesota vs. Carter*, 525 U.S. 83, 97 (1998), e si ricorda l'opinione concorrente di Scalia).

"In aggiunta, il test di Katz si basa sull'assunto che questa ipotetica ragionevole persona è giunta a un insieme ben sviluppato e stabile di aspettative sulla privacy. Ma la tecnologia può cambiare queste aspettative. Un drammatico mutamento tecnologico può condurre a periodi in cui le aspettative popolari sono in flusso e può alla fine produrre cambiamenti significativi nelle attitudini popolari. La nuova tecnologia potrà portare una maggiore convenienza o sicurezza, a spese della privacy, e molte persone potranno trovare questo scambio conveniente. E sebbene la gente possa respingere questa diminuzione della privacy che la tecnologia porta con sé, essa potrebbe comunque finire per trovare questo sviluppo inevitabile" (*op. cit.*, 10, dove Alito rimanda allo studio pubblicato dall'autorevole *National Public Radio* (NPR) su "la morte della privacy": v. sopra § 6.2.3).

Nel mettere alla prova il test di Katz, le "nuove intrusioni alla privacy" provocate dall'innovazione tecnologica suggeriscono pertanto, a giudizio di Alito, uno scenario simile a quanto visto più sopra proprio a proposito del caso Katz (v. § 7.2.4); quando, si ricorderà, poco dopo la decisione della Corte, il Congresso intervenne a disciplinare organicamente la materia delle intercettazioni elettroniche con *The Omnibus Crime Control and Safe Street Act*. Con le parole di Alito e sia pure "in un senso ironico, benché *Katz* abbia corretto *Olmstead*, ciò che asseriva il *Chief Justice* Taft in quest'ultimo caso si è dimostrato essere vero, e cioè che la disciplina delle intercettazioni è una materia che sarebbe bene lasciare al Congresso […] Un corpo legislativo è bene collocato per misurare il mutamento delle attitudini pubbliche, per definire linee ben precise e bilanciare la privacy con la sicurezza pubblica in un modo comprensibile" (*op. cit.*, 11 e 13).

Ciò non significa evidentemente che, in attesa dell'intervento del legislatore, la Corte non possa dirimere i casi; anzi, a differenza dell'opinione maggioritaria predisposta da Scalia, l'opinione di Alito, Ginsburg, Breyer e Kagan, ritiene che sia il test di Katz, e non certo quello del *trespass* o dell'intrusione fisica, a spiegare perché Jones abbia avuto ragione. Mentre, nei precedenti della Corte, il monitoraggio a breve termine dei movimenti di una persona sulle pubbliche vie è stato ritenuto compati-

bile con una ragionevole aspettativa di privacy, invece, "l'uso di un più lungo termine di controllo tramite GPS nelle investigazioni sulla maggior parte dei delitti lede queste aspettative" (*op. cit.*, 13). È proprio il punto sul quale, a sua volta, Scalia si sofferma in senso critico nella decisione della Corte, sottolineando l'incertezza che si verrebbe in questo modo a creare con un duplice criterio sia temporale sia parametrato alla gravità dei delitti: "non c'è alcun precedente per la tesi che, per stabilire se un'intrusione sia avvenuta, bisogna investigare la natura del delitto perseguito. E, anche accettando questa novità, rimarrebbe da spiegare perché una investigazione di quattro settimane sia 'sicuramente' troppo lunga e perché la cospirazione del narco-traffico, concernente grosse somme di denaro e narcotici, non sia un 'crimine straordinario' che non possa permettere una più lunga sorveglianza. Perché non due giorni di controllo per un sospetto di furto di elettronici? O sei mesi di sorveglianza per un sospetto terrorista?" (*op. cit.*, 12).

D'altra parte, la disparità di vedute tra i giudici va completata con le ulteriori osservazioni di Sonia Sotomayor. La *Justice* riprende infatti le osservazioni del collega Alito, sul fatto che "l'intrusione fisica non sia ora necessaria per condurre svariate forme di sorveglianza" e che "lo stesso progresso tecnologico che ha reso possibile tecniche di sorveglianza non intrusive sul piano fisico, inciderà sul test di Katz, nel rimodellare l'evoluzione delle aspettative sociali di privacy" (565 U.S. _, pp. 2-3). Sotomayor accoglie sostanzialmente l'opinione di Alito che la sorveglianza a lungo termine tramite l'uso della tecnologia GPS, abbia leso la ragionevole aspettativa di privacy nel caso Jones, "perché il monitoraggio GPS costa poco se paragonato alle tecniche di sorveglianza convenzionale e, per il suo stesso design, agisce surrettiziamente, sottraendosi ai controlli consueti che limitano l'esercizio abusivo del dovere di far rispettare la legge" (*ibidem*). Inoltre, c'è da sospettare, con una vecchia preoccupazione della giurisprudenza della Corte suprema, che la consapevolezza di poter essere sorvegliati dal Governo può violare, o mettere a repentaglio, le libertà dei cittadini, per quanto riguarda l'ulteriore libertà di pensiero e parola (v. §§ 7.2.1 e 7.2.3). Di qui, davanti allo scenario di un governo legittimato a registrare, tramite GPS, tutte le tracce dei movimenti degli individui, *justice* Sotomayor si domanda, retoricamente, "se la gente ragionevolmente si attenda che i propri movimenti siano registrati e aggregati in maniera tale dal Governo che esso possa stabilire, più o meno, le credenze politiche e religiose, gli abiti sessuali e così via" (*op. cit.*, 4).

Tuttavia, c'è un ulteriore motivo per ricordare in questa sede le parole di *justice* Sotomayor: si tratta di quell'accezione della privacy come controllo che è stata discussa, introducendo il capitolo precedente, con la figura 18, e che è forse giunto il momento di rivedere. In alternativa ai dubbi costituzionali di Alito, Sotomayor sottolinea infatti come, "più fondamentalmente, potrebbe essere necessario riconsiderare la premessa che un individuo non abbia una ragionevole aspettativa di privacy per quanto riguarda l'informazione che si è volontariamente dischiusa ai terzi" (p. 5). A ben vedere, "questo approccio mal si adatta all'età digitale, in cui la gente rivela una grande parte della propria informazione personale a terze parti, nel corso di rapporti quotidiani. La gente svela ai propri fornitori di servizi i numeri telefonici che compongono o i testi per sms; gli indirizzi web che visitano o gli indirizzi di email […] e i libri, generi alimentari e medicine che acquistano dai rivenditori in rete" (*ibidem*). Probabilmente, ripensando ai dubbi del giudice Alito, si può temere

che dal riposizionamento tecnologico in corso, nel campo della privacy, potrà seguirne un gioco al ribasso, in cui gli individui accetteranno "meno privacy" per più servizi in cambio, o più sicurezza, "o forse no […] Ma – avverte Sotomayor – qualunque siano le aspettative sociali, esse possono assurgere al rango di diritti costituzionalmente protetti, soltanto se il nostro orientamento sul Quarto Emendamento smette di trattare la segretezza come un prerequisito per la privacy"; ossia, secondo quella accezione della privacy come limitazione, rappresentata dalla figura 18 del sesto capitolo.

Da questo punto di vista, il giudice della Suprema sembra propendere per una concezione della privacy come accesso ristretto e controllo limitato: abbandonando la logica proprietaria del tutto o niente, o della privacy come "bene discreto", bisogna piuttosto considerarla secondo la logica abituale per cui "uno svela certi fatti a una banca o a una compagnia telefonica con uno scopo commerciale ben definito, senza assumere che questa informazione sia per ciò svelata ad altre persone per altri scopi".

Nondimeno, conclude Sotomayor la propria opinione, la "risoluzione di queste difficili questioni non è necessaria in questo caso, perché l'intrusione fisica del Governo nella Jeep di Jones fornisce una base più ristretta per la decisione. Pertanto, mi unisco all'opinione maggioritaria [della Corte presieduta da Scalia]".

## 7.5. *Una ragionevole aspettativa di privacy*

Abbiamo ripercorso nelle pagine precedenti l'evoluzione del Quarto emendamento nella giurisprudenza della Corte suprema per quasi un novantennio; ossia, dall'opinione dissenziente di Brandeis in *Olmstead* (1928), alla nuova dottrina, fondata sul concetto di privacy, nel caso Katz (1967), fino all'applicazione del test ivi formulato dal giudice Harlan nei casi a venire, soprattutto da Kyllo (2001) a Jones (2012).

In rapporto agli osservabili della figura 22, abbiamo così esaminato come la privacy sia tutelata in luoghi pubblici e a casa propria, nonché tra le due sfere, come una nuova sorta di privacy digitale che, di tanto in tanto, finisce per intrecciarsi con l'ulteriore forma di protezione della privacy, all'insegna del Primo emendamento, come libertà di parola.

Inoltre, riportando le varie opinioni dei giudici della corte, ci siamo soffermati anche sul loro diverso giudizio circa il test sulla ragionevole aspettativa di privacy: mentre, per alcuni, il test può essere reso superfluo dalla protezione contro intrusioni illecite approntata dalla tradizione di common law (Scalia); per altri, invece, può essere difficile risolvere i nuovi casi della rivoluzione informatica sulla base del test (Alito); oppure, bisognerebbe in realtà rivedere queste stesse basi (Sotomayor).

In questo paragrafo, l'intento è di tirare le somme dell'analisi sul test, alla luce delle opinioni della Corte suprema americana, sintetizzando il dibattito in ragione di tre punti principali: la "natura circolare" del test (§ 7.5.1); i suoi limiti politici (§ 7.5.2); e ciò che, nondimeno, possiamo imparare ancora dal test medesimo (§ 7.5.3).

### 7.5.1. *Circolarità*

Esistono due "circoli" che ben si prestano a riassumere il dibattito attorno al test sulla ragionevole aspettativa di privacy: il circolo "virtuoso" e quello "vizioso".

Nel primo caso, il riferimento va al ponte che s'instaura tra leggi formali e norme sociali, mediate dalla iurisdictio, nel momento di definire cosa sia costituzionalmente legittimo, o meno, nell'ordinamento federale americano, a proposito dell'insieme di concetti etichettati come privacy sotto l'egida del Quarto emendamento. Attraverso il test bisogna appurare se un individuo abbia mostrato, o meno, in un caso determinato, l'aspettativa di tenere taluni suoi comportamenti, azioni o pensieri, per sé e, cioè, privati. Non ci sarebbe bisogno di passare al secondo punto del test, se tale individuo avesse agito in "luoghi aperti", se avesse partecipato tali informazioni a terzi, e così via. Solo qualora l'aspettativa di un individuo di vedersi riconosciuta la tutela della propria privacy sia acclarata dal suo comportamento, è necessario passare al secondo punto del test, per considerare se la società sia pronta a riconoscere o meno come ragionevole, quella stessa aspettativa. Nel caso in cui la risposta a quest'ulteriore domanda sia positiva, di modo che l'aspettativa soggettiva debba andare protetta con il Quarto emendamento, s'innescherebbe un circolo virtuoso tra individuo, società e sistema giuridico: l'aspettativa di tutela individuale, attraverso la mediazione della iurisdictio, troverebbe corrispondenza nelle norme sociali della comunità che, a loro volta, finiranno per essere rinforzate dal vedere garantita l'attesa di tutela individuale da parte dell'ordinamento.

Tuttavia, come riferito nel paragrafo precedente con l'opinione concorrente del giudice Alito nel caso Jones, si può scorgere nella struttura del test un circolo vizioso, più che virtuoso. L'aspettativa di privacy da parte dell'individuo può infatti essere tutelata costituzionalmente, soltanto a condizione che la società sia pronta a riconoscerla come ragionevole; ma, allora, delle due l'una. O l'opinione della società che quell'aspettativa individuale sia ragionevole, è contraddetta dal fatto che la lite verta proprio sulla legittimità dell'aspettativa nel caso considerato; oppure, l'aspettativa individuale è per davvero costituzionalmente protetta, nel qual caso è inutile rifarsi alla seconda parte del test. Si tratta, in fondo, del vecchio dilemma se sia nato prima l'uovo, o la gallina, che, in ambito giuridico, torna spesso a proposito della natura delle consuetudini come fonte normativa del sistema (v. §§ 2.2 e 4.1). Riassunta secondo la formula latina dell'*opinio iuris ac necessitatis*, la ragione per cui un individuo ritiene doveroso (*necessitas*) comportarsi in un determinato modo, dipende dal motivo (*opinio*) che la maggior parte dei consociati si comporti proprio in quel modo determinato. Ma, allora, viene prima l'*opinio* o il comportamento materiale dei consociati?

In realtà, abbiamo riferito fin dal capitolo secondo, alcune delle modalità secondo cui emergono dalla complessità dell'interazione sociale, fenomeni d'ordine spontaneo come, appunto, nel caso delle norme consuetudinarie (§ 2.2.2). Passando dai temi della sociologia (sia pure del diritto) al piano del diritto costituzionale, rimane però il problema di prendere posizione nella fase di emersione di quegli ordini spontanei. Il test sulla ragionevole aspettativa di privacy può infatti alimentare un circolo vizioso per tre ragioni differenti: in primo luogo, si può negare che ci sia una ragionevole aspettativa da parte di un individuo, proprio perché la società sta anco-

ra maturando la propria *opinio* al riguardo. In questo caso, il test innescherebbe un gioco al ribasso, dato che la censura della corte, nei confronti dell'irragionevole aspettativa individuale, finirebbe per incidere sulla stessa incertezza che la società ha sul riconoscere, o meno, quella aspettativa come ragionevole.

In secondo luogo, si può contestare, come nota del resto Alito nella ricordata opinione nel caso Jones, che sono sempre e solo i giudici della Corte suprema a dover stabilire cosa la società sia pronta a riconoscere come ragionevole. Lungi dall'innescare un circolo virtuoso tra individuo, società e sistema giuridico, il test sarebbe un comodo artificio con cui i giudici possono legittimare qualsivoglia decisione essi prendano. Nel caso in cui essi respingano le richieste del ricorrente, ciò significherebbe che la società non è pronta al riconoscimento e, viceversa, nel caso di accoglimento delle richieste, che tale riconoscimento è avvenuto. Mancherebbe pertanto il vincolo normativo delle norme sociali cui si era rifatto il giudice Harlan nella formulazione originaria del test, dato che il riconoscimento delle attese individuali di privacy non dipenderebbe tanto da ciò che i consociati pensano, ma da come i giudici ritengono (o retoricamente fanno finta) che i consociati pensino.

In terzo luogo, il test sarebbe palesemente inadeguato proprio in un'epoca, come la nostra, in cui, per dirla ancora con Alito (§ 7.4.1.1), le aspettative popolari sono "in flusso" per via della rivoluzione informatica e, anzi, molto spesso gli individui non sanno, o non avrebbero consapevolezza su come le proprie decisioni e azioni, a contatto con le nuove tecnologie, finiranno per ripercuotersi sulla loro stessa aspettativa di privacy. Del resto, abbiamo avuto in questo capitolo la riprova dell'accelerazione nello sviluppo tecnologico, riassunta con la legge di Moore (§ 1.3), a conferma del flusso di queste aspettative. Mentre, nei primi paragrafi del capitolo, ci siamo a lungo soffermati sui problemi giuridici posti dalla tecnologia del telefono, a un certo punto, a partire dagli anni ottanta, si è osservato come le sfide giuridiche della tecnologia si siano moltiplicate a ritmo crescente. Si è passati dall'uso degli aerei e dei satelliti in *Dow Chemical* (§ 7.2.4); ai sensori termici in *Kyllo* (§ 7.3.1); al GPS e a tutti i nuovi congegni della sorveglianza elettronica discussi in *Jones* (§ 7.4.1.1). Davanti ai nuovi scenari della "quarta rivoluzione" – questa la conclusione di molti, anche negli Stati Uniti d'America – sarebbe il caso che intervenisse il gubernaculum a fissare i parametri di cosa possa intendersi come una ragionevole aspettativa di privacy ai giorni nostri.

### 7.5.2. *Decisioni politiche*

Si è già detto come il giudice Alito, nell'opinione concorrente nel giudizio del caso Jones, abbia richiamato il precedente di Katz, non solo per applicare il test al nuovo caso; ma per sottolineare, in dissenso con l'opinione maggioritaria della Corte, che il gubernaculum, più che la iurisdictio, è spesso l'organo che si trova nelle condizioni migliori per definire le linee normative generali che disciplinano una data materia: nello specifico, il bilanciamento tra privacy e pubblica sicurezza (§ 7.4.1.1). Nel caso Jones, significativamente, a conforto della propria opinione, Alito citava gli studi di un giurista alla George Washington University, Orin Kerr (n. 1971), il quale, più volte, ha avuto modo d'insistere sul punto. In *The Fourth Amendment and New Technologies*, ritroviamo quella nozione di "flusso" che, nel

2012, Alito riprende per spiegare la sua tesi. Con le parole di Kerr, "le corti dovrebbero puntare in favore della cautela giudiziaria quando la tecnologia è in flusso, e dovrebbero considerare di lasciare al potere legislativo il compito di fornire le norme primarie che disciplinano l'intreccio tra le investigazioni delle forze dell'ordine e l'impiego di nuove tecnologie […] Quando la tecnologia è in flusso, le protezioni del Quarto emendamento dovrebbero rimanere relativamente modeste, fino a quando la tecnologia non si stabilizzi" (Kerr 2004: 805).

A conferma della disparità di opinioni presenti oggi in America e tra i giudici della Corte di Washington, la questione è tornata a porsi il 25 giugno 2014, nei casi *Riley vs. California* e *United States vs. Wurie*, allorché la Suprema si è espressa sul sequestro dei cellulari da parte della polizia e se le forze dell'ordine possano acquisire le informazioni contenute nello *smartphone* di una persona arrestata, senza il mandato previsto dal Quarto emendamento (v. 573 U.S. _). Da un lato, secondo il parere di *justice* Roberts, c'è una differenza abissale tra il modo in cui la polizia provvede normalmente a perquisire le tasche di una persona arrestata e il fatto che le forze dell'ordine possano impossessarsi del cellulare di quell'individuo, cominciando a rovistarne il contenuto. "I telefoni cellulari si distinguono da ogni altro oggetto che possa avere con sé l'arrestato, sia in senso quantitativo che qualitativo. Il termine 'telefono cellulare' è perfino fuorviante: molti di questi apparecchi sono infatti piccoli computer cui capita di essere impiegati anche come telefoni. Essi potrebbero altrettanto facilmente essere chiamati telecamere, riproduttori video, agende, registratori, archivi, diari, album, televisori, mappe interattive o giornali" (*op. cit.*, 17). La straordinaria capacità di memoria degli odierni cellulari solleva perciò problemi inediti per la tutela della privacy, in quanto i diversi tipi d'informazione contenuta in quel cellulare non soltanto svelano molte più cose di quanto ogni singolo dato informativo possa fare isolatamente, ma i dati possono risalire indietro nel tempo per parecchi anni ed essere immagazzinati in *server* remoti. Davanti alle tesi del Governo che l'ispezione dei dati racchiusi nei cellulari sono "materialmente indistinguibili" dalle perquisizioni che si fanno sugli oggetti fisici delle persone arrestate, *justice* Roberts ha buon gioco nel replicare che "ciò è come dire che un giro a cavallo è materialmente indistinguibile da un viaggio sulla luna. Entrambi sono modi per giungere dal punto A al punto B, sebbene poco altro giustifichi la similitudine" (*ibidem*). Di qui, salvo casi particolari, in cui le forze di polizia ritengano che il cellulare possa ad esempio essere impiegato come detonatore, la conclusione maggioritaria della Corte non è che "l'informazione su un telefono cellulare sia immune da ricerche; piuttosto, un mandato è di norma richiesto prima dell'ispezione, anche quando il telefono sia stato messo sotto sequestro dopo un arresto" (*op. cit.*, 25).

D'altra parte, sono proprio questi casi particolari – e i precedenti citati a sostegno dalla Corte – che hanno spinto *justice* Alito a presentare, dopo Jones, un'altra opinione concorrente. Pur d'accordo sulle novità dei problemi insorti nell'era digitale, Alito contesta il bilanciamento tra privacy e sicurezza cui si è giunti nel caso *Riley*, perché, estendendo le garanzie del Quarto emendamento a tutte le informazioni contenute su qualsiasi cellulare, "questo approccio comporta alcune anomalie" (373 U.S. _ 4). Basti pensare a due sospetti: il primo con in tasca la bolletta del telefono e la lista delle chiamate fatte, alcune delle quali incriminatrici, oltre a qualche fotografia altrettanto compromettente. L'altro sospetto con in tasca un cellulare

con la lista di chiamate e foto in memoria, che potrebbero rivelarsi ugualmente fatali. "Stando alla legge oggi vigente, la polizia potrebbe sequestrare ed esaminare la bolletta del telefono e le foto nelle tasche [del primo sospetto] senza mandato, ma a seguire il parere espresso oggi dalla Corte, ciò sarebbe precluso per l'informazione contenuta in un telefono cellulare" (*op. cit.*, 5). In realtà, osserva Alito, "mentre concordo con il parere della Corte, sarei pronto a riesaminare la questione se il Congresso, oppure la legge di uno Stato [dell'Unione], dopo aver considerato i bisogni legittimi delle forze dell'ordine e gli interessi alla privacy dei proprietari di cellulari, approvasse una normativa con una serie di distinzioni ragionevoli fondate sul tipo d'informazione e forse altre variabili" (*ibidem*). Nel riprendere le argomentazioni esposte nel caso Jones, Alito nota così come "molte forme della tecnologia moderna rendono sempre più facile al governo e a enti privati di ammassare una quantità d'informazione sulla vita di ogni americano e, allo stesso tempo, molti di questi americani scelgono di rendere pubblica una massa d'informazione che, soltanto poche decadi fa, difficilmente sarebbe stata svelata ad estranei. Alla luce di questi sviluppi, sarebbe proprio una disgrazia se la protezione della privacy nel XXI secolo dovesse soprattutto dipendere dal giudizio delle corti federali con l'arma spuntata del Quarto emendamento. I corpi legislativi, eletti dal popolo, sono in una posizione migliore della nostra, per valutare e rispondere ai cambi che sono già avvenuti e a quelli che quasi certamente avranno luogo in futuro" (*op. cit.*, 6).

In fondo, non è la prima volta in questo libro che, esaminando il rapporto tra le fonti del sistema e, in specie, tra gubernaculum, iurisdictio e consuetudini, osserviamo come il baricentro si sposti – o vada spostato – sul piano del potere legislativo.

Innanzitutto, abbiamo visto come le norme sociali e gli ordini spontanei del kosmos ben possano inoltrarsi per vicoli ciechi, per ciò stesso richiedendo l'intervento del legislatore: v. §§ 2.2.2.1, 3.3.2 e 5.2.1. Secondo i criteri normativi approntati nel capitolo terzo, vero è che il legislatore, in taluni casi, è tenuto ad argomentare le ragioni del proprio intervento (§ 3.4.3.1); ma, da tale onore della prova non segue affatto che la suddetta azione sia inutile in un numero copioso di casi. Anzi, proprio affrontando le controversie sorte per via dell'innovazione tecnologica – come quelle esaminate in questo capitolo – abbiamo sottolineato le diverse opzioni che il legislatore ha davanti a sé, quando deve intervenire in questo ambito (§ 5.3.1). In fin dei conti, non siamo forse venuti dicendo fin dal capitolo primo che il diritto e, per traslato, il gubernaculum, tra esecutivo e legislativo, possono essere convenientemente rappresentati all'insegna di una meta-tecnologia? (§ 1.1.3).

Inoltre, si è anche riferito come il ruolo della iurisdictio non sia quello di sostituirsi ai compiti del gubernaculum; ma, piuttosto, di esserne il contrappeso istituzionale, come organo di controllo: §§ 3.2.1 e 6.2.4. Dopo tutto, abbiamo visto in questo capitolo come il Congresso di Washington sia dovuto intervenire per porre rimedio agli esiti di una sentenza della Corte suprema che, vuoi per l'idiosincrasia dei suoi giudici, vuoi per il tenore della legge, sono stati ritenuti insoddisfacenti (§ 7.2.4). Il risultato è che spesso, in via fisiologica, non può che essere il gubernaculum a fissare le norme del diritto attraverso le leggi. Si tratta di un approccio su cui si è già insistito nel capitolo precedente, introducendo le differenze specifiche tra il modello statunitense e quello europeo nel settore della privacy (§ 6.3.3). In quella sede, si è riferito come, nell'Unione europea, principi e norme sulla protezione dei

dati personali sono fissati dal Parlamento e dal Consiglio congiuntamente, e poi garantiti dal controllo diffuso dei giudici nazionali che trovano nella giurisprudenza della Corte di Lussemburgo il proprio riferimento ultimo. Nel caso degli Stati Uniti, invece, l'idea di "lasciare al legislativo il compito di fornire le norme primarie", per dirla ancora con Orin Kerr, non ha tanto a che fare con la disciplina del rapporto tra privati, per cui vale il principio dell'autonomia individuale e dell'auto-regolamentazione delle società d'affari con codici di condotta. Piuttosto, secondo la tradizione di quel paese, l'urgenza dell'intervento del gubernaculum, emersa da ultimo con il caso Riley, suggerisce che il Congresso fissi quanto prima per legge un chiaro bilanciamento tra individuo e stato, tra privacy e sicurezza pubblica.

Dal raffronto tra la vocazione generale del modello europeo della privacy e quella settoriale dell'approccio americano, in molti sono giunti alla conclusione che la maggior parte delle questioni che assillano il dibattito odierno negli USA, possono essere affrontate con profitto, avendo a mente proprio l'esperienza che l'Europa è venuta nel frattempo maturando al riguardo. Basti menzionare che, già nel 2004, il direttore del programma per la tecnologia e la libertà dell'*American Civil Liberties Union* (ACLU) – ossia una delle più importanti associazioni americane per la tutela dei diritti civili – Barry Steinhardt, ha dichiarato che "non dobbiamo chiedere all'Europa di adeguarsi al nostro modello, ma piuttosto noi adeguarci al loro" [7].

Ma, anche ad ammettere che le odierne questioni di privacy chiamino soprattutto in causa l'intervento del gubernaculum e, lungo questa via, che il modello europeo di protezione dei dati possa essere utile per affrontare alcuni problemi del modello statunitense, sorge per ciò stesso la domanda: che fine fa la dottrina della ragionevole aspettativa di privacy elaborata dalla Corte suprema? Il test, in altri termini, diventa inutile con l'intervento puntuale del legislatore? O, come sostenuto da *justice* Sotomayor nella sua opinione concorrente nel caso Jones, sono le stesse basi del test che richiedono di essere riviste?

### 7.5.3. *Viaggio in Europa (con biglietto di ritorno)*

Abbiamo riferito nel corso dei capitoli precedenti come l'Unione europea vanti un'esperienza ventennale in materia di trattamento e protezione dei dati personali; e, cioè, a partire dalla direttiva 46 del 1995 in avanti. Si tratta con ogni evenienza di un settore che, pur intrecciandosi necessariamente con quello della privacy, non va confuso con questo: prova ne sia che, nell'introduzione del capitolo sesto, abbiamo ricordato come la Carta dei diritti fondamentali dell'Unione europea distingua accuratamente la tutela dei dati personali di cui all'articolo 8, dall'articolo 7 che, con formula associabile alla lettera del Quarto emendamento, si occupa del "diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni".

Questo doppio piano di tutela risulta particolarmente rilevante perché una delle peculiarità che segnano l'evoluzione del modello statunitense della privacy in tema di Quarto emendamento, consiste precisamente nel fatto che, per via delle sollecita-

[7] La dichiarazione è reperibile presso *http://www.aclu.org/privacy/spying/15032prs20040202.html*.

zioni del progresso tecnologico, anche questa tutela ha finito più spesso per identificarsi con la disciplina relativa alla protezione sul trattamento e uso dei dati personali nelle odierne società ICT-dipendenti. Se, nel presente capitolo, abbiamo seguìto l'evoluzione alla luce dei precedenti della Corte suprema, da Olmstead a Riley, abbiamo anche detto come il Congresso di Washington sia del pari corso ai ripari; e, sia pure, con una serie di interventi settoriali (§ 6.1.2). L'esame del modello europeo per la protezione dati può di qui essere un utile punto di riferimento per chiarire molti dei bivi decisionali, su cui si ritrova a discutere oggi il legislatore nordamericano, stante la vocazione generale che ha viceversa ispirato l'approccio europeo. Ad esempio, l'annotazione di *justice* Sotomayor, per cui occorrerebbe rivedere la tradizionale "regola della divulgazione a terzi" (§ 7.4.2), è stata ormai da tempo acquisita in Europa, a proposito delle finalità e modalità che rendono legittimo il trattamento dei dati, sulla base del consenso, per un periodo di tempo determinato. Analoghe considerazioni valgono per l'indebita identificazione di privacy e segretezza, frequente negli USA, secondo una tesi ormai largamente screditata in Europa.

Tuttavia, nell'accingerci a introdurre nel prossimo capitolo il modello europeo della protezione dati, occorre muovere da una avvertenza che, poi, riconduce all'attualità del test elaborato nell'ultimo mezzo secolo dalla Corte suprema. La disciplina, anche molto dettagliata, dei principi e regole che devono governare il settore della protezione dati in Europa, non sembrerebbe lasciare spazio al test sulla ragionevole aspettativa nel vecchio continente, dato che simile aspettativa sarebbe, appunto, fissata dalla serie di direttive che il legislatore europeo è venuto approvando nel corso degli ultimi due decenni. Eppure, come diventerà man mano evidente, studiando il modello europeo, tanto i suoi limiti e difetti, quanto l'incidere del progresso tecnologico, finiranno per riportare alla ribalta quel test nato, quasi per caso, con le telefonate di Mr. Katz a metà degli anni sessanta. La tesi che si vuole sostenere è che occorra recuperare quel nesso tra norme sociali e leggi formali che la fitta rete di provvedimenti e, finanche, qualche sentenza al di qua dell'Atlantico tendono invece a svalutare o screditare.

# VIII.
# *Protezione dati*

> "Ciò che intendiamo per informazione (per unità elementare di informazione) è una differenza che produce una differenza"
>
> Gregory BATESON

Il settore del trattamento e tutela dei dati personali rappresenta uno degli ambiti del diritto, in cui lo sviluppo della tecnologia e la "quarta rivoluzione" si palesano nel modo più chiaro. Sul piano storico, abbiamo riferito come tra gli anni sessanta e settanta dello scorso secolo, per via della crescente diffusione delle banche dati, al vecchio diritto alla privacy si sia venuta affiancando l'esigenza di tutela di un nuovo autonomo diritto, ossia, la protezione dei dati personali (§ 6.1.2). Sul piano filosofico, tale riposizionamento tecnologico della privacy in chiave informazionale ha reso sempre più evidente come i termini chiave del discorso giuridico, quali diritti, garanzie o sanzioni, riguardino più spesso l'accesso e controllo sul flusso dell'informazione nel nuovo ambiente che, fin dal capitolo primo, abbiamo indicato come "infosfera" (§ 1.4). Ciò che la "quarta rivoluzione" mette bene in mostra, è infatti la nostra natura di organismi informazionali interconnessi: essendo, più che avendo, informazione, è ragionevole pensare a una qualche forma di difesa.

Rispetto alla tutela tradizionale della privacy, la protezione dei dati personali presenta tre caratteristiche peculiari: in primo luogo, il riferimento va ai "dati", piuttosto che alle "informazioni", secondo la distinzione già appurata nel capitolo secondo (§ 2.1). In quella sede, per chiarire la nozione d'informazione semantica basata su dati dotati di significato, si è parlato di dati come mancanza di uniformità nel mondo reale. La tutela accordata già solo ai dati, piuttosto che alla dimensione informativa della privacy, sta perciò a suggerire una più ampia e diversa protezione, proprio perché si ha di mira ogni mancanza di uniformità nel mondo reale, a cui però possiamo attribuire potenzialmente un significato determinato.

In secondo luogo, il bene giuridico che si mira a proteggere – ciò che il Tribunale costituzionale tedesco definisce come il "diritto all'auto-determinazione informativa" degli individui – crea una corrispondente nuova serie di obblighi in capo a coloro che trattano, usano e riusano i dati personali nell'era dell'informazione. Se, con la vecchia privacy, il dovere era soprattutto quello di "non fare", come nel caso classico di non farsi gli affari degli altri, con il nuovo diritto alla protezione dei dati, spesso, sorge un obbligo corrispondente di "fare" in capo al responsabile del trattamento. Tornando alle linee guida dell'OCSE, si tratterebbe della specificazione

dei fini del trattamento, con le misure di sicurezza, la raccolta limitata dei dati, ecc. (v. § 6.3.2).

In terzo luogo, il regime della protezione dei dati ha di mira la trasparenza con cui l'informazione personale è processata lungo il suo intero ciclo di vita: dal momento della raccolta, anche in tempo reale, dei dati, alla loro eventuale cancellazione senza back-up. La normativa in materia di protezione dei dati protegge di qui, solo indirettamente, quella opacità delle persone, ossia il loro non dover essere del tutto trasparenti agli altri; che, con Hannah Arendt, abbiamo visto essere la prima preoccupazione dell'istituto (§ 6). Ciò non significa che la tutela della privacy e la protezione dei dati personali non possano sovrapporsi: basti pensare che le norme sul trattamento e uso dei dati personali devono, per molti versi, essere intese non solo come regolatrici del flusso con cui le informazioni circolano nell'ambiente; ma anzi, come norme che vincolano quel medesimo flusso informativo per garantire l'"opacità" delle persone.

Nondimeno, il baricentro dell'attenzione giuridica viene in questo modo spostato dalla tradizionale tutela della ragionevole aspettativa di privacy da parte di un individuo, alla nuova tutela della trasparenza con cui il dato è raccolto, trattato e usato. Ne segue un necessario bilanciamento tra la maggiore garanzia che viene accordata all'individuo, nell'anticipare la soglia di tutela dall'informazione (privacy) al dato (personale); ed evitare che la nuova generazione di leggi a tutela della raccolta e uso dei dati possa tuttavia creare una sorta di feticcio. Avremo più volte occasione di illustrare tale rischio nel corso delle prossime pagine: è il caso del funzionario che non rilascia un documento, adducendo fantasiosi motivi di privacy; è il caso di come evitare che innumerevoli riusi legittimi dell'informazione nel settore pubblico (PSI) siano vanificati dalla scusa della protezione dati, ecc. Sono gli eccessi che, a parti invertite, il lettore avrà sperimentato, nel momento di dover automaticamente firmare una clausola di liberatoria sulla privacy per avere una stanza di albergo, o la macchina in "car sharing", oppure al momento di far click sulle clausole che regolano i termini del servizio su una piattaforma sociale (*social network*).

Al fine di comprendere come operi concretamente questo riposizionamento dal bene giuridico dell'opacità nei termini consueti della privacy al fine della trasparenza nel settore della protezione dati, il capitolo è suddiviso in cinque parti. A continuazione (§ 8.1), l'attenzione andrà al "modello europeo" della privacy e, più in particolar modo, a questioni di sovranità (§ 8.1.1), diritti umani (§ 8.1.2), diritto alla personalità (§ 8.1.3), e se sia configurabile in Europa un nuovo *habeas data*, a complemento del tradizionale *habeas corpus* (§ 8.1.4). Sebbene avremo occasione di riferirci anche ad altri sistemi giuridici, come la tutela della privacy in Brasile o in Argentina, inizia così il nostro esame di un modello, quello europeo della tutela dei dati personali, che propone per molti versi un'alternativa a quanto fin qui detto in rapporto al modello statunitense della privacy.

Più in particolar modo (§ 8.2), verranno analizzati i quattro baluardi su cui poggia il regime di trattamento dati in Europa: la sua qualità (§ 8.2.1), il principio del consenso (§ 8.2.2), il piano delle garanzie (§ 8.2.3), e quello della protezione (§ 8.2.4). Dopo di che (§ 8.3), prenderemo in considerazione le modalità d'uso: per così dire la dinamica, più che la statica, del sistema. Per comprendere come i quattro baluardi del trattamento dati interagiscano, l'esempio sarà dato dai termini consensuali del servizio tra privati (§ 8.3.1).

Una volta che i dati siano legittimamente raccolti, essi saranno per lo più usati e riusati (§ 8.4): di qui, che occorra far caso a come il diritto alla protezione dei dati concorra con l'esercizio di una pletora d'altrui diritti, come il diritto di parola, di libertà d'espressione, di cronaca, d'informazione, e così via. Vengono esaminati cinque casi: il rapporto tra dati personali e apertura dei dati (§ 8.4.1), il loro uso personale (§ 8.4.2), commerciale (§ 8.4.3), e per la sicurezza (§ 8.4.4), con il relativo regime di ritenzione dei dati (§ 8.4.5).

Questo affresco generale è completato con il regime di responsabilità, secondo la tradizionale tecnica "se A, allora B", dove le sanzioni "B" sono rappresentate dalle misure previste a carico sia dei responsabili per il trattamento dei dati, sia degli individui che li usano e che, tuttavia, non abbiano ottemperato ad "A" (§ 8.5). Con la tradizione, ci si soffermerà ora sui casi di responsabilità penale degli individui, come responsabilità personale (§ 8.5.1); ora sulla responsabilità civile (§ 8.5.2). Su queste basi, potremo apprezzare il ruolo svolto dal regime giuridico di immunità per i fornitori di servizi in rete (§ 8.5.2.1-2). Si tratta di una disciplina che ha fin qui accomunato tanto il modello europeo, quanto quello statunitense, e che, pertanto, introduce idealmente la serie di problemi con cui i due modelli sono attualmente alle prese e, soprattutto, le ulteriori questioni con le quali saremo chiamati a fare i conti nei prossimi anni. Lasciando al prossimo capitolo l'esame di questi ultimi temi sul futuro della privacy, cominciamo a capire la natura giuridica dell'ambito relativo al trattamento e alla tutela dei dati personali, a partire dall'esame del modello europeo.

## 8.1. *Il modello europeo*

Prima ancora di entrare nel dettaglio del modello europeo con le modalità di raccolta e trattamento dei dati, principi di riuso, responsabilità, sicurezza ecc., occorre coglierne le caratteristiche principali. Ciò consente di precisare perché si parli di modello e quali siano le specificità nei confronti di altri e ulteriori paradigmi, come quello nordamericano.

Quattro differenze balzano subito all'occhio: esse sono illustrate con i nuovi osservabili dell'analisi di cui alla figura 23:

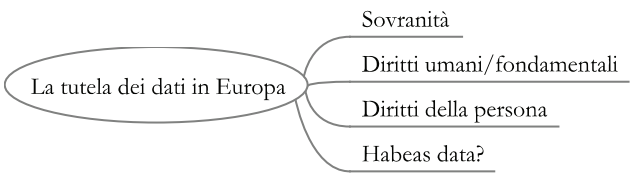


Figura 23: *Il modello europeo di privacy*

Il primo osservabile riguarda il fatto, già segnalato (§ 4.3.2.1), per cui l'Unione europea non dispone della "competenza della competenza" e, soprattutto in settori come la difesa e l'ordine pubblico, si ha una distribuzione dei poteri sensibilmente diversa a quanto accade nell'ordinamento statunitense. Per via della sovranità degli

stati membri dell'Unione europea, in altri termini, tali stati riservano gelosamente a sé i poteri per garantire ciò che abbiamo indicato come "l'opposto aristotelico" della privacy, ossia, la sicurezza nazionale (§ 6.2). Per ora, non esiste qualcosa di simile al Quarto emendamento nel diritto europeo contemporaneo.

Il secondo osservabile mette in mostra un'ulteriore differenza tra i due modelli: a differenza della tutela settoriale che viene accordata negli Stati Uniti (§ 7), sia il diritto alla protezione dei dati personali, sia il diritto alla privacy, sono posti alla base del costrutto dell'Unione europea. La distinzione che la figura 23 fa tra diritti umani e diritti fondamentali sottolinea un'ulteriore caratteristica del modello: la tradizionale tutela del diritto alla privacy nei confronti dei poteri sovrani degli stati, secondo l'articolo 8 della Convenzione europea del 1950, è affidata alla Corte dei diritti umani di Strasburgo sul piano del diritto internazionale. La chiusura del sistema relativa alla tutela dei dati personali e della vita privata nell'Unione è affidata invece alla Corte di Lussemburgo, nelle forme e limiti previsti dal diritto UE (§ 4.3.2.1).

Il terzo osservabile completa il precedente: non soltanto il diritto alla tutela dei dati personali, al pari del diritto alla privacy, è un diritto fondamentale nell'Unione europea, ma esso va riferito ai diritti della personalità degli individui, piuttosto che alla tutela della loro proprietà. Qui si trova un'altra basilare differenza tra i due modelli, dato che, viceversa, negli Stati Uniti, l'idea corrente è che uno "abbia" – e non "sia" – le proprie informazioni. Ne consegue che molte delle disposizioni europee nell'ambito della protezione dei dati abbiano natura inderogabile, a differenza del più flessibile approccio americano basato per lo più sul consenso delle parti.

In ragione della natura fondamentale e personale che il diritto alla tutela dei dati ha nell'Unione europea, ciò porta infine a indagare se si possa propriamente parlare di un *habeas data* nel vecchio continente. Sin dai tempi dell'*habeas corpus* medioevale, il tema tuttavia s'intreccia con le garanzie che l'individuo deve avere nei confronti del potere sovrano; riportando, per questo verso, al primo osservabile dal quale siamo partiti. Per procedere con ordine, nell'indagine degli osservabili della figura 23, conviene pertanto tornare al principio di sovranità nel modello europeo e capire come funzioni in questo contesto la competenza della competenza.

### 8.1.1. *Sovranità*

A partire dalla prima normativa comunitaria in materia di privacy, la ricordata direttiva 46 del 1995, la tutela europea dei dati personali ha incontrato due limiti genetici: il primo è fissato dal secondo punto dell'artico 3 di quella direttiva, per cui essa non si applica al trattamento di dati che hanno per oggetto la sicurezza nazionale, la difesa o l'ordine pubblico, oltre alle attività dello Stato in materia penale e al benessere economico che s'intreccino indissolubilmente a ragioni o motivi di sicurezza. Questo significa che, nella ripartizione di competenza tra Unione e stati membri, questi ultimi, in nome della propria sovranità, hanno tenuto per sé la gestione di questo lato cruciale del sistema giuridico.

Il secondo profilo genetico è invece chiarito dall'articolo 13 della direttiva, che specifica i limiti o eccezioni al funzionamento del diritto comunitario nell'intreccio tra mercato unico e diritti fondamentali della persona. Le norme del diritto comunitario possono essere sospese, sia pure secondo una procedura che prevede l'assenso

della Commissione, in sette circostanze: quando occorre garantire la "sicurezza dello Stato" vera e propria (art. 13.1 lettera (a)), la "difesa" (b), la "pubblica sicurezza" (c), nel caso d'"infrazioni penali o di violazioni della deontologia delle professioni regolamentate" (d), per "un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria" (e), per compiti variamente collegati all'esercizio dei pubblici poteri di cui alle precedenti tre lettere della legge (f), e, infine, quando si tratti della "protezione della persona interessata o dei diritti e delle libertà altrui" (g).

Ad onor del vero, presentando nel gennaio 2012 la proposta di un nuovo regolamento per la protezione dei dati in Europa, la Commissione ha anche illustrato il disegno di una nuova direttiva per la protezione dei dati nei settori della polizia e della giustizia penale[1]. Nel settimo considerando della proposta, si legge che "il livello della protezione dei diritti e delle libertà degli individui riguardo al trattamento di dati personali da parte delle autorità competenti ai fini della prevenzione, investigazione, detenzione o perseguimento dei delitti o l'esecuzione delle sanzioni penali […] dev'essere equivalente in tutti gli Stati Membri". Inoltre, aggiunge la Commissione, "la protezione dei diritti e libertà dei titolari dei dati […] richiede misure, tecniche e organizzative, in grado di garantire che le finalità della presente direttiva siano raggiunte. Per assicurare che le previsioni della presente direttiva siano ottemperate, il responsabile [dei dati] dovrà adottare strategie e implementare misure appropriate, tali da soddisfare, in particolare, i principi della protezione dei dati tramite design e come configurazione base" dei sistemi informativi (n. 38 della proposta di direttiva).

Anche a dar retta all'organo europeo, bisogna tuttavia aggiungere come, sempre nel gennaio 2012, chiarendo questa volta la proposta per sostituire la direttiva 46 con un nuovo regolamento, il documento della Commissione riproduca all'articolo 2 quanto detto, in sostanza, con il vecchio articolo 3. Per quanto si armonizzi lo scambio di informazioni tra le forze dell'ordine in Europa, sulla base di un alto standard di tutela come auspicato dalla Commissione nella direttiva per la polizia e la giustizia penale, siamo infatti ben lungi dal quadro normativo esaminato nel capitolo precedente. Lì, le decisioni della Corte suprema avevano per oggetto la tutela della privacy degli individui nei confronti del governo o degli stati dell'Unione; qui, al contrario, la disciplina introduce una serie sistematica di eccezioni nei confronti del settore pubblico, rispetto al quadro generale previsto per le relazioni tra privati, che la Corte di giustizia dell'Unione è chiamata a tutelare. Per trovare qualcosa di vagamente analogo al laborioso impegno della Corte di Washington e la sua ermeneutica del Quarto emendamento, bisogna considerare la giurisdizione della Corte di Strasburgo e i casi da essa decisi sul piano del diritto internazionale, in rapporto all'articolo 8 della Convenzione europea dei diritti dell'uomo (§ 5.4.3).

Passiamo, in questo modo, al secondo osservabile della figura 23.

[1] Il riferimento va a COM(2012) 10 finale 2012/0010 (COD).

### 8.1.2. *Diritti umani*

Abbiamo ricordato nel capitolo quarto (§ 4.3.2.1), come la Corte di giustizia sia venuta tutelando i diritti umani nell'ordinamento comunitario sin dai primi anni settanta, nonostante quel sistema giuridico non fornisse, allora, alcun conforto testuale; e come, nondimeno, sia sorto sin d'allora uno scontro, mai sopito, tra la Corte di Lussemburgo e altre corti supreme nazionali, come nel caso del Tribunale costituzionale tedesco. Per tutelare, come fondamentale, un diritto non scritto, la Corte europea si è valsa in quelle prime decisioni, come *Internationale Handelsgesellschaft* (1970), *Nold* (1974), e poi *Hauer* (1979), del criterio ermeneutico che fa leva sui principi generali del diritto. La corte ha infatti sostenuto che la tutela dei diritti umani costituisce "parte integrante" del diritto comunitario, richiamandosi alle tradizioni costituzionali comuni degli stati membri e, in parte, alla Convenzione europea dei diritti dell'uomo. Ciò non ha scalfito né i dubbi di chi, ora come allora, fa fatica a rinvenire queste tradizioni comuni tra paesi così diversi come l'Italia o il Regno Unito, né le preoccupazioni di chi, giudice di una corte suprema in uno stato membro, si pone il problema di un possibile conflitto tra le proprie decisioni e quelle della Corte di giustizia dell'Unione a proposito di diritti fondamentali.

Tuttavia, nel caso della tutela dei dati personali da parte della Corte di giustizia, i suoi compiti sono in misura rilevante circoscritti dai due limiti genetici dell'approccio comunitario, evidenziati nel paragrafo precedente. Ciò comporta nel settore specifico della protezione dei dati che, per quanto ci possa essere incomprensione tra la Corte di giustizia e i tribunali nazionali costituzionali, questa incomprensione non riguarda alcune delle decisioni chiave che gli stati membri prendono in materia di difesa e sicurezza nazionale, mantenimento dell'ordine pubblico ed esercizio dell'azione penale. Questa consistente sfera dell'ordinamento non è stata infatti affidata alla tutela della Corte di Lussemburgo, come guardiana dei trattati dell'Unione, poiché, come riferito (§ 5.4.3), la Corte si occupa piuttosto della tutela dei dati personali tra privati e delle relative eccezioni per il settore pubblico. Come diremo (§§ 8.4.4 e 8.4.4.1), ciò non significa che la Corte di giustizia non debba mai entrare nel merito di controversie che riguardino la disciplina dell'ordine pubblico o la sicurezza nazionale; ma è indicativo che, anche o soprattutto in questi casi, la Corte richiami espressamente, in via analogica, le pronunce dei colleghi di Strasburgo.

Per ritrovare, invece, al centro della iurisdictio, la tutela della privacy in rapporto alle misure che gli stati prendono per la difesa o sicurezza o mantenimento dell'ordine pubblico, bisogna considerare i sistemi giuridici di ciascun stato membro dell'Unione con i propri anticorpi istituzionali. Da questo corollario del principio di sovranità discende che sarebbe difficile parlare di un modello europeo su questo punto, date le differenze anche rimarchevoli che esistono non solo, o non tanto, tra gli ormai circa trenta stati membri dell'Unione, ma finanche tra gli stati membri della vecchia comunità economica europea, come il Regno Unito e la Grecia, la Svezia o l'Italia. Avendo tutti gli stati europei sottoscritto la CEDU del 1950, esiste naturalmente un comune quadro di riferimento che fa capo alla giurisprudenza della corte di Strasburgo, alla quale qualunque individuo potrà rivolgersi nel caso in cui, esauriti i gradi di giudizio nel proprio sistema giuridico, egli ritenga sia stato violato il diritto di cui all'articolo 8 della Convenzione.

Ma, per quanto encomiabile sia stato il lavoro svolto dalla CEDU negli ultimi 60 anni, chiaro è che la robustezza della tutela del diritto non possa essere la stessa svolta dal supremo organo giurisdizionale del diritto del proprio paese: è sufficiente ricordare come facciano parte della CEDU sia la Russia che la Turchia, per cogliere le ragioni del perché il quadro normativo della CEDU, messo a confronto con le garanzie costituzionali di alcuni stati come il Regno Unito o la Norvegia, appaia come una sorta di minimo comune denominatore di tutela, o *extrema ratio*, per gli individui che si oppongono alle pretese assicurative dei propri stati. Il dato suggerisce che possiamo propriamente parlare di un modello europeo per quanto concerne la tutela dei dati personali all'interno degli stati membri dell'Unione, ma sarebbe improprio identificarlo con il sistema europeo che è viceversa sorto per la tutela della privacy nel quadro della CEDU. Entrambe le varianti dell'approccio europeo si distinguono nondimeno dalle forme in cui ora la privacy, ora la protezione dei dati, sono pensate in America. Si tratta del terzo osservabile della figura 23, per cui il modello europeo mette a fuoco il tema come una forma di tutela inerente alla persona, più che alla proprietà, dell'individuo.

### 8.1.3. *Privacy come diritto della personalità*

Il terzo osservabile della figura 23 illustra una fonte continua d'incomprensioni tra esperti al di qua e al di là dell'Atlantico: mentre la tutela dei dati personali, al pari di quella della vita privata degli individui, è per lo più rubricata tra i diritti della personalità negli ordinamenti degli stati membri dell'Unione, invece, negli Stati Uniti, vige per lo più un approccio fondato sul consenso e l'autonomia delle parti, che fa leva sul diritto di proprietà per dirimere le controversie dell'interazione sociale. Come riferito (§ 6.1.2), l'esperienza del totalitarismo e diverse forme di autoritarismo hanno forgiato in Europa una nozione di privacy imperniata sulla dignità delle persone, come avviene ad esempio nella Costituzione federale tedesca del 1949 o con l'articolo 2 della Costituzione italiana, in questo senso contrapponibili alla tradizionale rappresentazione in chiave fisica e proprietaria della tutela offerta negli USA dal Quarto emendamento. Per chiarire ulteriormente il punto, basta accennare alla fondamentale sentenza che il Tribunale costituzionale tedesco ha emesso il 15 dicembre 1983, nota come *Volkszählungs-Urteil* o "decisione sul censo".

In quella sede, i giudici di Karlsruhe erano chiamati a stabilire la legittimità costituzionale di diverse parti della legge federale sul censo del 1982, che finivano non solo per sovrapporsi alle norme introdotte nel 1977, proprio a tutela dei dati personali (v. § 6.1.2); ma, rischiavano di comprometterne l'impianto generale volto alla salvaguardia della personalità degli individui. Con le parole della corte, "un ordine sociale – e l'ordine giuridico che lo supporta – in cui i cittadini non siano più in grado di determinare chi conosce cosa su di essi, quando, con quali mezzi, sarebbe incompatibile con il diritto all'auto-determinazione informazionale. Chiunque abbia il dubbio che il proprio comportamento dissenziente possa essere registrato in qualsiasi momento e immagazzinato permanentemente sotto forma di informazione, tenterà di non attrarre l'attenzione tramite tale comportamento. Ciò osterebbe non solo alle possibilità di sviluppo personale degli individui, ma anche al bene pubblico, poiché l'auto-determinazione è un prerequisito per un ordine politico libero, basato

sulla capacità di azione politica e collaborazione dei propri cittadini" (v. Glorioso 2012: 389).

Stabilendo l'illegittimità costituzionale di diverse parti della legge sul censo, che violavano il nuovo diritto all'auto-determinazione informazionale, la pronuncia del Tribunale di Karlsruhe avrebbe rappresentato negli anni a venire un punto di riferimento indiscusso anche per la nuova normativa che il legislatore comunitario avrebbe approntato con la direttiva 46 del 1995. Il nuovo diritto all'auto-determinazione informazionale come base per lo "sviluppo personale degli individui" e "prerequisito per un ordine politico libero", si sarebbe tradotto nel diritto di stabilire, in una serie nutrita di casi, se i dati personali possano essere raccolti ed, eventualmente, trasmessi a terzi; nel diritto di determinare se quei dati possano essere utilizzati e trattati; nel diritto di avere accesso a quei dati e, se del caso, aggiornarli; fino al diritto di cancellare quei dati e di rifiutare, in qualunque momento, di vedere quei dati trattati. A differenza dell'approccio che, almeno idealmente, va dal basso verso l'alto, sulla base del consenso e con la fiducia tra le parti, tipico del modello statunitense che disciplina il rapporto tra i privati, la politica del legislatore comunitario si è invece ispirata a un robusto approccio dall'alto verso il basso, sia pure temperato dall'apertura ai codici di condotta (§ 4.3.3.1). Anche ad assumere come pietra di paragone l'intervento federale del Congresso di Washington e la giurisprudenza della Corte suprema, spiccano le differenze con il quadro generale dei principi inderogabili e dei diritti indisponibili predisposto dal Parlamento e il Consiglio di Bruxelles.

Questo approccio è stato non di rado tacciato di paternalismo; e anche il più acceso sostenitore delle istituzioni europee dovrebbe ammettere che, in fondo, ci sia stato a volte un eccesso di zelo da parte del legislatore comunitario. Basti pensare a come, sin dalla prima direttiva del 1995, la normativa di Bruxelles abbia posto limiti rigorosi al trattamento di quel particolare tipo di dati personali che sono detti "sensibili", perché attinenti ad alcune informazioni particolarmente delicate sulla salute, razza, preferenze sessuali, e altro, degli individui. Il particolare regime di tutela di questi dati, per molti versi più che ragionevole, ha tuttavia condotto a effetti indesiderati: è stato il caso di alcune ricerche scientifiche che hanno dovuto aggirare i vincoli dell'articolo 8 D-95/46/CE, per poter svolgere i propri studi su come si diffondano i virus biologici, più che informatici, e su come formalizzarne la dinamica attraverso i modelli della teoria delle reti (§ 2.2.2). Per avere informazioni su quando un volontario si ammala in un certo periodo della ricerca, occorrerebbe infatti il consenso scritto ed espresso dell'interessato. Si dà però il caso che, a seguire alla lettera i vincoli della legge, quest'ultima finirebbe per rendere quasi impossibile la ricerca e, comunque, molto meno snella di quanto sarebbe fattibile, ottenendo quei dati dalla pagina di un *social network* grazie a un manipolo di volontari che informano quando hanno avuto il raffreddore. Attivandone la segnalazione su dove e quando chi tra questi volontari si è venuto ammalando durante la ricerca, quest'ultima, svolta attraverso una pagina di Facebook e con buona pace dell'articolo 8 della direttiva comunitaria, ha potuto così chiarire nel 2012 alcune delle leggi che regolano gli spostamenti e la diffusione dei virus, e a quale velocità[2].

[2] Per motivi di privacy, va da sé, non posso svelare chi abbia in questo modo condotto una, peral-

Del resto, questi effetti indesiderati della normativa europea nulla tolgono all'obiettivo di affrontare le sfide dell'impatto tecnologico sulla tutela della privacy con un nuovo diritto della personalità. A scanso di equivoci, bisogna insistere sul fatto che, declinato come diritto all'auto-determinazione informativa degli individui, oppure come versione aggiornata del principio dell'*habeas corpus*, il diritto alla protezione dei dati personali rappresenta un crocevia per difendere i restanti diritti e libertà costituzionali. Si tratta di un'idea per molti versi adombrata da Brandeis (§§ 6.1.1 e 7.2.1); e che, oltre al Tribunale costituzionale tedesco, ha trovato nuovi e convinti fautori anche nei paesi sudamericani. La natura sia fondamentale che personale del diritto alla protezione dei dati conduce di qui al quarto e ultimo osservabile della figura 23: l'opportunità di ripensare alla protezione dei dati personali secondo il vecchio e venerando principio dell'*habeas corpus*.

### 8.1.4. *Verso un habeas data?*

Il principio dell'*habeas corpus* risale agli albori del costituzionalismo medioevale inglese, tra il 1200 e il 1300, come meccanismo di garanzia processuale contro ogni forma di detenzione arbitraria. In sostanza, la persona imprigionata, o qualcuno al posto di essa, poteva (e può) richiedere un ordine (*writ*), con il quale il giudice di Sua maestà stabilisce l'udienza di comparizione delle parti, per appurare perché quell'individuo sia stato privato della sua libertà.

Nel corso dei secoli, il principio è stato adottato da tutti gli ordinamenti che si ispirano agli ideali dello stato di diritto della tradizione costituzionale moderna che trae origine dal common law: l'*Habeas Corpus Amendment Act* venne approvato dal Parlamento di Westminster nel 1679, e il principio nuovamente sancito con la gloriosa rivoluzione culminata con il *Bill of Rights* del 1689 e l'*Act of Settlement* del 1701.

Negli Stati Uniti, i Padri fondatori menzionano il principio all'articolo primo della Costituzione (sezione nona, clausola seconda), per cui "il privilegio del *writ* di *habeas corpus* non potrà essere sospeso, se non per casi di ribellione o quando la sicurezza pubblica lo richieda".

In Italia, il principio lo ritroviamo nell'articolo 13 della Costituzione del 1948.

Più recentemente, con l'incidere della rivoluzione informatica, è nata l'idea di integrare questa tradizionale tutela della persona fisica dell'individuo con una nuova forma di tutela della persona elettronica di ogni soggetto. Mentre, a partire dai primi anni ottanta, come visto nel paragrafo precedente, il Tribunale costituzionale tedesco è venuto affinando l'idea di tutelare la persona elettronica con il principio dell'auto-determinazione informativa degli individui, altri ordinamenti hanno espressamente fatto menzione del concetto di *habeas data*, al momento di varare le loro nuove costituzioni. Quella brasiliana del 1988, ad esempio, si richiama al diritto di *habeas data* "per garantire la conoscenza dell'informazione relativa alla persona del richiedente, contenuta in banche dati o archivi delle agenzie del governo o di natura pubblica" e "per la correzione dei dati". A sua volta, l'articolo 43 della Costituzione

---

tro, legittima ricerca scientifica: si tratta di un tipico esempio del diritto all'anonimato previsto dalla tutela del Primo emendamento!

argentina del 1994 sancisce che "ogni persona potrà esperire ricorso per ottenere informazione sui dati che la riguardano e i loro scopi, custoditi in archivi pubblici o banche dati, o in enti privati volti a fornire informazione; e nel caso in cui i dati siano falsi o discriminatori, questo ricorso potrà richiedere la soppressione, rettifica, confidenzialità o aggiornamento dei predetti dati. La natura segreta delle fonti giornalistiche d'informazione non dovrà essere messa a repentaglio".

Si ricorderà, citato all'inizio del capitolo sesto, l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea (2000), secondo cui gli individui hanno un diritto alla tutela dei dati personali che fa perno su due criteri: quello che il trattamento avvenga secondo il principio di lealtà, per finalità determinate e sulla base del consenso, e quello che ogni individuo abbia il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne, se del caso, la rettifica. Questo insieme di tutela va poi garantito sul piano della iurisdictio, nel senso che "il rispetto di tali regole è soggetto al controllo di un'autorità indipendente" (articolo 8.3 della Carta). Per le ragioni dette (§ 8.1.2), molto della tutela effettiva del principio di *habeas data* in Europa si gioca però, ancora, nella sfera della sovranità gelosamente custodita dagli stati membri dell'Unione. Questo ha indotto, in certi casi, a segnalare come un vero e proprio *habeas data* non esista nel modello europeo di tutela della privacy; altre volte, che sia il caso di lavorare nondimeno in questa direzione (v. Rodotà 2006). A ben vedere, si tratta di un processo tuttora in divenire se, con la proposta della Commissione per un nuovo regolamento europeo sulla tutela dei dati personali, nel gennaio 2012, ferve ancora il dibattito su quali ulteriori diritti, e doveri, debbano essere fissati per legge.

A prescindere dall'esito che potrà mai avere quest'ultimo dibattito, sembra chiaro che l'asse portante del modello europeo non ne uscirà comunque modificato. Sul piano del diritto UE, esiste di già una robusta protezione della persona elettronica degli individui, specialmente nel rapporto tra i privati, che funge da quadro generale entro cui inserire una serie di limiti o eccezioni, in omaggio al principio della sovranità degli stati membri. Sono i limiti di cui agli articoli 3 e 13 della direttiva 46, fino all'articolo 2 del nuovo regolamento della Commissione (v. § 8.1.1).

Possiamo ora passare all'analisi, nel dettaglio, della via europea all'*habeas data*.

## 8.2. *I principi del trattamento*

La normativa europea in materia di dati personali, a differenza di quella settoriale americana, ha una vocazione generale, nel duplice senso che mira a regolare l'intero ciclo di vita dell'informazione e a prescindere dal particolare ambito, o tipo di rapporto, in cui quei dati sono raccolti e, poi, trattati.

Abbiamo fin qui visto come per questa tutela, prima in sede giurisprudenziale, con la decisione sul censo del Tribunale costituzionale tedesco, e in séguito per legge con la direttiva comunitaria, si sia venuta introducendo una nuova generazione di diritti nel nome dell'auto-determinazione informativa individuale: il diritto di rifiutare che i dati siano trattati in determinate circostanze, il diritto di libero accesso ai dati medesimi, fino alla capacità di modificare e di eliminare, se del caso, i dati. Questi diritti vanno raccordati alla serie di obblighi posti a capo dei soggetti che a

loro volta raccolgono, trattano e, magari, rivendono quei dati a terzi. Il rapporto tra il titolare dei dati e il responsabile per il loro trattamento si presenta così come un insieme di diritti e di doveri, che possono, in questa sede, essere riassunti sulla base di quattro punti principali. Essi riguardano la qualità del trattamento dei dati (§ 8.2.1); il consenso degli interessati (§ 8.2.2); le garanzie per alcune classi particolari di dati, come quelli sensibili (§ 8.2.3); e, infine, la sicurezza dei dati tra il settore pubblico e quello privato (§ 8.2.4).

Queste sono le basi che rappresentano, per così dire, la statica del sistema: una volta presa familiarità con i principi del trattamento, esamineremo come tali principi interagiscano in concreto, con le modalità d'uso di quei dati (§ 8.3).

### 8.2.1. *Qualità*

Abbiamo definito nel capitolo quinto (§ 5.3.1), la nozione di trattamento dei dati che va ora completata con quella di dato personale. Nel modello europeo della privacy, fin dall'articolo 2 D-95/46/CE, la nozione va intesa come qualsiasi tipo di informazione che identifichi, o renda identificabile, una persona fisica o "naturale". Il trattamento dei dati personali deve così rispettare una serie di principi, il primo dei quali è riassunto con la formula sulla "qualità dei dati", tanto dal vecchio articolo 6 della direttiva, quanto dall'articolo 11 del codice italiano sulla privacy (§ 6.2.2).

La formula della qualità riguarda sia le modalità del trattamento, sia gli scopi, sia il rapporto tra finalità e dati raccolti, sia la correttezza di questi ultimi fino alla fine dello stesso trattamento. La figura 24 illustra i nuovi osservabili e variabili dell'indagine:

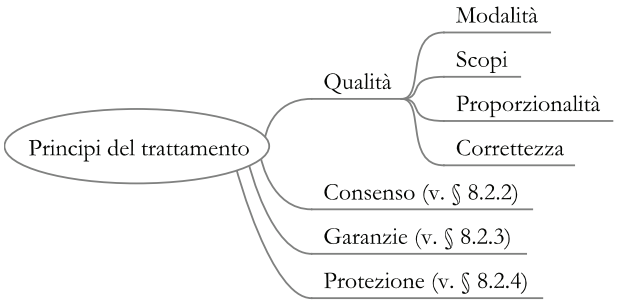


Figura 24: *La qualità del modello*

Più in particolar modo, per quanto riguarda le modalità del trattamento, il modello prevede la clausola generale che detto trattamento sia leale, ai sensi dell'articolo 8 della Carta dei diritti fondamentali dell'Unione; e che sia inoltre lecito, e cioè rispetti gli ulteriori obblighi e doveri posti a carico di chi provvede a raccogliere e trattare dati personali.

In secondo luogo, gli scopi per i quali è richiesto, o comunque si provvede a, trattare i dati, devono essere espliciti e specifici: il titolare dei dati deve in altri termini essere in condizione di sapere per quali fini i suoi dati sono trattati.

In terzo luogo, i dati raccolti dovranno essere rilevanti rispetto alle finalità per-

seguite e, comunque, non eccedenti riguardo a tali finalità: si tratta del principio di proporzionalità applicato alla qualità del trattamento, per cui la richiesta di dati deve essere appunto proporzionata alle ragioni di quel trattamento.

Infine, i dati trattati dovranno essere esatti e, se del caso, modificati e aggiornati, fino a quando le informazioni non siano più strettamente necessarie al conseguimento dei risultati, per i quali i dati sono stati raccolti e, poi, trattati.

I dati trattati secondo gli standard di qualità ora detti, possono essere processati legittimamente a condizione di soddisfare un ulteriore principio del modello; quello che stabilisce cioè quando – più che come – i dati potranno essere trattati. La tecnica del legislatore europeo è stata quella d'individuare, nel consenso, il concetto sul quale incardinare questo secondo principio per il trattamento dei dati. Dopo di che, seguono le eccezioni del caso, per le quali il consenso, dunque, non è più necessario, ma valgono comunque le regole sulla qualità del trattamento esaminate in questo paragrafo.

### 8.2.2. *Consenso*

La regola generale che rende legittimo il trattamento dei dati personali, è data dal consenso "inequivocabile" della persona interessata. Questo consenso, beninteso, deve essere informato: ciò significa che l'individuo deve avere le informazioni necessarie per comprendere le finalità per cui i dati sono raccolti; e sapere chi sono i responsabili del trattamento dei dati, i destinatari o le categorie dei destinatari per i quali i dati sono trattati, e se rispondere alle domande sia obbligatorio o meno. In caso di diniego, inoltre, l'interessato deve essere a conoscenza delle conseguenze per l'eventuale mancata risposta e, comunque, come possa esercitare il diritto di accesso o rettifica rispetto ai dati che lo riguardano. Soltanto su queste basi, e cioè con il via libera del diretto interessato, si può procedere al trattamento dei dati raccolti con le forme viste nel paragrafo precedente.

Tuttavia, fin dalla prima direttiva del 1995, esiste una vistosa serie di eccezioni alla regola generale del consenso. Benché nelle forme leali del trattamento stabilite dall'articolo 8 della Carta dei diritti fondamentali, il consenso non è richiesto:

a) per l'adempimento di accordi contrattuali dell'interessato;
b) per le sue obbligazioni;
c) per la salvaguardia di un suo interesse vitale;
d) per l'esecuzione di un compito pubblico o connesso all'esercizio di pubblici poteri;
e) per il perseguimento di un interesse legittimo.

Il principio dell'auto-determinazione informativa degli individui trova così limiti che si fondano, ora, su una precedente auto-determinazione (lettera a); ora, sulla tutela della stessa persona (lettera c); ora, nel contemperamento con altri interessi (lettere b ed e); ora, nel tipico bilanciamento con il fine di garantire la sicurezza pubblica (lettera d), su cui siamo più volte tornati nel corso di queste pagine come l'"opposto aristotelico" della privacy (§ 6.2).

Anche con questi limiti, nondimeno, il consenso rimane la chiave di volta per rendere legittimo il trattamento di una massa sterminata di dati personali che sono,

poi, quelli che gli individui riversano volontariamente, in forma quotidiana, sulle piattaforme sociali; o portano con sé, direttamente, sui propri cellulari.

Qui, bisogna però fare un'ulteriore distinzione tra la protezione riservata ai dati personali e quella relativa a una particolare classe di dati personali e, cioè, i dati sensibili. La distinzione non solo serve a precisare le modalità secondo cui il consenso informato dell'individuo deve essere richiesto (e ottenuto) in taluni casi; ma, richiama anche l'attenzione su come il trattamento di questa particolare classe di dati personali richieda maggiore attenzione per le misure di garanzia e sicurezza. Secondo il tenore dell'articolo 8 della direttiva 46, si tratta di "dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale". Nel corso del paragrafo seguente, vedremo come questa classe di dati incida sulle modalità e ragioni che rendono lecito il trattamento.

### 8.2.3. *Garanzie*

La tecnica del legislatore comunitario nel disciplinare il trattamento dei dati sensibili è la stessa seguíta per la disciplina del consenso: s'introduce la supposta regola generale – in questo caso, quella che vieta in linea di principio il trattamento che riguardi l'origine razziale o l'etnia delle persone, le loro opinioni politiche e sindacali, le proprie convinzioni etiche e filosofiche, nonché i dati relativi alla salute o alla vita sessuale – per poi introdurre una serie di deroghe ed eccezioni. Esse concernono:

a) i dati relativi ai rapporti di lavoro;
b) la ricerca scientifica;
c) il trattamento dei dati sanitari;
d) i casellari giudiziari;
e) il registro delle condanne penali.

Specie per quanto riguarda questi ultimi tre punti, il modello prevede che gli stati membri dell'Unione, salvo notifica alla Commissione delle proprie decisioni, godano di un ampio margine di discrezionalità nel disciplinare la raccolta e uso dei dati. Per esempio, sono gli stati che stabiliscono se e a quali condizioni i numeri nazionali d'identificazione, come nel caso delle carte di identità, siano oggetto di trattamento. Inoltre, davanti alla liberatoria dell'interessato per la diffusione di dati relativi alla sua origine, salute e vita sessuale, opinioni politiche, convinzioni religiose o appartenenze sindacali, spetta sempre allo stato stabilire per legge l'eventuale insufficienza del consenso prestato (articolo 8.2 lettera (a) della direttiva 46 del 1995).

Questa discrezionalità degli stati si applica anche alle misure di sicurezza: avendo presente la natura dei dati sul registro delle condanne penali, o nei casellari giudiziari, così come rispetto al sistema del trattamento dei dati sanitari, non solo è richiesto un "livello appropriato rispetto ai rischi presentati dal trattamento" – come recita l'articolo 17 di quella direttiva – ma, proprio per la natura di quei dati, devono essere gli stati a stabilire se, per esempio, i trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza, come anche nel caso di dati riguardanti sanzioni amministrative o procedimenti civili, possono essere effettuati solo sotto controllo dell'autorità pubblica; o se "per motivi di interesse pubblico rilevante" gli

stati possano fissare ulteriori deroghe nella gestione e controllo dei dati concernenti il mondo del lavoro e i servizi sanitari nazionali. In parte, come s'è visto precedentemente (§ 8.1.1), l'ordinamento dell'Unione tende ad armonizzare anche questi settori tradizionalmente riservati alla sovranità degli stati membri, come nel campo della polizia e la giustizia penale. Oltre a ragioni di efficienza e garanzia nella tutela dei dati personali, come nel caso del sistema di Europol, l'armonizzazione è però stata favorita anche dai rischi che più spesso si sono presentati nel trattamento di questi dati.

In termini generali, i rischi legati al trattamento dei dati sensibili, hanno consigliato una particolare tutela delle modalità e condizioni relative al trattamento stesso: prendendo ad esempio il codice della privacy in Italia, l'articolo 20 prevede la riserva di legge per il trattamento di dati sensibili da parte di soggetti pubblici, l'articolo 23 la forma scritta del consenso dell'interessato, l'articolo 26 garanzie per il trattamento dei dati sensibili, anche senza il consenso dell'interessato, tramite autorizzazioni del Garante, ecc. Su questo impianto generale, è andato poi a innestarsi l'ulteriore impatto del progresso tecnologico che, specie nel campo della biometria e con l'identificazione degli individui per mezzo del DNA, ha consigliato a molti l'idea di differenziare ulteriormente tra dati sensibili e dati sensibilissimi. Dal punto di vista dei principi, riguardo alle condizioni di raccolta, trattamento e uso di questi dati, non cambia molto rispetto all'impianto già pensato per la tutela dei dati sensibili: la forma scritta del consenso, le restrizioni all'accesso a quei dati da parte di terzi, le autorizzazioni delle autorità garanti, e così via. Piuttosto, l'attenzione va rivolta alle particolari modalità secondo cui tali dati devono essere protetti: si tratta di un tema discusso già a partire dal capitolo quinto, quando, a proposito di misure di sicurezza, si è distinto tra *safety* e *security* (§ 5.2.2). Occorre ora riprendere questo discorso, a proposito della protezione dei dati personali sensibili o meno.

### 8.2.4. *Protezione*

Il tema della sicurezza nel trattamento dei dati personali rappresenta uno dei suoi capitoli più rilevanti e significativi: è sufficiente menzionare che l'intero titolo quinto della parte generale del codice sulla privacy in Italia è dedicato appunto alla sicurezza dei dati e dei sistemi informativi (ICT), con un apposito allegato in materia di "misure minime".

A sua volta, sin dalla prima direttiva, all'articolo 17, l'ordinamento comunitario si è occupato del "fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati". Inoltre, come recita il considerando 46 di quella stessa direttiva, il legislatore comunitario ha proclamato il fine di perseguire questo obiettivo – di prevenire cioè la distruzione, perdita o accesso non autorizzato dei dati – con l'approccio che poi sarebbe diventato popolare con il nome di "privacy tramite design" (§§ 5.4.3 e 6.2.4).

Così, fin dal 1995, l'intento dichiarato è stato di avvalersi della tecnologia per pervenire a un alto standard di qualità nella protezione dei dati, secondo quelle modalità, introdotte nel capitolo quinto, relative alla "funzione promozionale" del design (§ 5.2.1), e allo sviluppo di "airbag digitali" (§ 5.2.2). Con l'intento d'incoraggiare gli individui a cambiare comportamento, o proteggerli dall'impatto di even-

ti dannosi, abbiamo visto come il disegno dei sistemi e la configurazione degli interfaccia informatici, i dispositivi di recupero (back up), e ulteriori accorgimenti come password, sistemi d'identificazione all'accesso e uso dei dati, filtri di crittografia, ecc., possano effettivamente contribuire alla protezione dei dati, nel duplice senso di *safety* e *security*. In quest'ultimo caso, bisogna garantire la sicurezza del sistema, come sua condizione primaria, nel senso che il suo venir meno può mettere in condizione altri di arrecare danno, oppure rendere loro più agevole farlo. Nel pensare alla sicurezza come *safety*, l'accento cade invece sulla condizione il cui venir meno può recare un danno diretto o immediato agli interessati.

Gli investimenti tecnologici per la sicurezza rimangono tuttavia uno dei punti più controversi della disciplina, almeno dal punto di vista dei controllori e responsabili del trattamento dei dati, per i quali è evidente che queste misure di sicurezza hanno un prezzo. Allorché la Commissione europea ha presentato la proposta di regolamento nel gennaio 2012, una delle prime preoccupazioni per molti è stata quella di quantificare l'aumento dei costi che le misure annunciate, o minacciate, dalla Commissione, avrebbero comportato. Uno studio ha per esempio quantificato i costi del nuovo regolamento presentato dalla Commissione, stabilendo una perdita tra lo 0.3 e l'1.3% del prodotto interno lordo dell'Unione e, cioè, fino a 260 euro per cittadino (Lee-Makiyama 2014: 91). Ma, anche ad ammettere che tali costi siano in realtà un investimento – ed è, in effetti, dimostrato come una buona reputazione sul piano della sicurezza e tutela dei dati giovi alle imprese: si pensi alle banche online – rimane il fatto che le misure protettive richieste, a volte, possono essere sproporzionate. Valga sin d'ora il richiamo alle restrizioni previste nel caso del riuso delle informazioni del settore pubblico (§ 8.4); oppure, del trattamento dei dati sensibili come ostacolo al libero svolgimento d'indagini scientifiche (§ 8.1.3). Al costo delle misure di protezione stabilite dal legislatore, si assomma il mancato risparmio, o ritorno economico, reso possibile da un uso più che legittimo dei dati, che tuttavia, in nome della sicurezza, si finisce per impedire o intralciare.

D'altra parte, in forma eguale e contraria a questi limiti e come veniamo ripetendo dal capitolo primo (§ 1.4.1), le misure di sicurezza informatica sono a loro volta vulnerabili: lo si è visto con i sistemi di protezione per i contenuti informativi coperti dall'esclusiva della proprietà intellettuale (§ 5.4.2); e a contatto con i programmi nazionali per la sicurezza pubblica (§ 6.2.1). Se a questi esempi si aggiunge, poi, quello della criminalità in rete e il variegato mondo dei reati informatici (§ 1.4.2), non è difficile capire perché l'adozione delle misure di sicurezza per la protezione dei dati rappresenti uno dei punti più sensibili e dibattuti dell'intera normativa. A conferma, basti pensare che tra le novità più rilevanti della proposta di regolamento della Commissione, c'è il dovere di informativa in capo ai responsabili del trattamento, per cui, nel caso di falla nei sistemi di sicurezza informatica (*security*), essi sono tenuti ad avvertire gli utenti dei propri servizi (*safety*).

Finora, sulla base della direttiva 46 del 1995, si è verificato il classico caso dove la duplice esigenza di *safety* e *security* ha finito non di rado per condurre a finalità divergenti; e, cioè, da un lato, l'interesse dell'utente a veder protetti i propri dati personali (*safety*), e, dall'altro, l'interesse del gestore di un sistema informativo il cui sistema di sicurezza (*security*) sia stato perforato da un virus o un *cracker*. Nell'ipotesi in cui il responsabile del trattamento non sia tenuto a comunicare all'interessato il malaugurato

evento della perdita, distruzione o manomissione dei dati, è evidente come s'in-stauri un'indebita gerarchia tra la sicurezza (*security*) del sistema informativo e dei contenuti in esso immessi tramite il controllo sull'accesso ai dati, e la tutela della sicurezza (*safety*) dei dati personali. Con il venir meno della prima (*security*), finirebbe infatti per essere automaticamente sacrificata la seconda (*safety*). Mentre, fin qui, abbiamo esaminato alcuni modi in cui questi tipi di protezione sono stati più o meno bilanciati nell'ambito della sicurezza nazionale e pubblica (figura 21 del § 7), oltre alle decisioni della Corte di giustizia sulla legittimità di massicci sistemi di filtraggio in rete (§ 5.4.3), si tratta di approfondire a continuazione in che modo la duplice esigenza di *safety* e *security* con cui i dati devono essere raccolti e trattati, si posizioni nel rapporto tra privati.

Come diremo, rispetto alla consueta prospettiva che fa leva sul modello della "informativa e consenso", una particolare attenzione andrà alla nozione di rischio, che rimane tuttavia sottesa a quella delle misure di sicurezza e ai suoi costi. In tempi di vacche magre per l'Unione e il suo PIL, occorre saggiare la possibilità di rendere il modello più dinamico e flessibile.

### 8.3. *Le modalità d'uso*

Nelle pagine precedenti abbiamo indicato i quattro punti attorno a cui ruota il modello europeo sulla protezione dei dati personali: la qualità del trattamento, la regola del consenso, le garanzie per certi dati sensibili e i diversi modi in cui devono intendersi le misure di protezione. Insieme alle variabili della figura 24 del § 8.2.1, si sono precisati tre ambiti, in cui la raccolta e il trattamento dei dati personali, che pur devono ispirarsi al principio di lealtà, non dipendono dal consenso dell'interessato (§ 8.2.2); oppure, la raccolta è resa più difficile per la natura di quei dati, in quanto sensibili (§ 8.2.3); o, per motivi di sicurezza, i dati possono essere resi inaccessibili a terze parti. Nonostante queste restrizioni, all'atto pratico, la maggior parte dei dati personali raccolti o trattati sistematicamente su base quotidiana, avviene però di regola secondo la volontà degli stessi interessati, per cui uno "cede" i propri dati al fornitore di servizi in rete, o al gestore della telefonia, o al noleggiatore di auto, agli alberghi, ai supermercati o grandi magazzini, e così via. Dal punto di vista giuridico, questa è la forma ordinaria secondo cui il modello stesso dovrebbe funzionare e cioè, secondo la regola del consenso come fondamento di legittimità della raccolta e trattamento dei dati personali, a cui si affianca un numero ristretto (cinque) di eccezioni. Come funziona dunque, fisiologicamente, il modello?

Al riguardo, occorrerebbe almeno distinguere i rapporti tra imprese e singoli, sulla base di un accordo che definisce i termini del servizio, e i rapporti tra i singoli stessi, tramite i servizi di quelle imprese; oppure in proprio, attraverso tutti i mezzi messi a disposizione dalla rivoluzione informatica: email, chat, blog, ecc. Per molti versi, sono i differenti tipi di rapporto che definiscono i diversi livelli di responsabilità riguardanti il trattamento e la protezione dei dati personali, su cui torneremo diffusamente verso la fine del capitolo (v. § 8.5).

Per ora, limitiamoci a concentrare l'attenzione sulla prima delle ipotesi ora formulate, ossia su come funziona il modello europeo della protezione dati che disciplina il rapporto tra imprese e singoli, in ragione dei principi di lealtà del trattamento, consenso dell'interessato, garanzia per i dati e loro sicurezza.

### 8.3.1. *Servizio, termini e consenso*

Al pari del modello americano, anche quello europeo prevede che i rapporti tra imprese e singoli siano regolati dai loro accordi sui termini del servizio. A differenza, però, del modello americano, quello europeo prevede il rispetto di una nutrita serie di principi relativi al trattamento e tutela dei dati, per cui, al fine di un consenso informato, il fornitore dei servizi ha il dovere di chiarire all'interessato quali dati e per quali motivi vengano raccolti, se essi saranno o potranno essere trasmessi o ceduti a terze parti, quando verranno cancellati, ecc.

Lasciando in sospeso questa differenza tra Stati Uniti ed Europa, ciò che accomuna i due modelli è il fatto che da un punto di vista formale, come suol dirsi, "il contratto è legge tra le parti". Sono gli utenti che acconsentono ai termini di uso e trattamento dei loro dati personali, predisposti dai fornitori del servizio, per telefonare su Skype, mandare messaggi su WhatsApp e Twitter, postare su Facebook, caricare video su YouTube, e via dicendo. Mentre è innegabile che questi servizi abbiano contribuito a riplasmare la vecchia aspettativa di privacy in modo considerevole, perché il modo in cui i dati personali vengono caricati e usati negli ambienti elettronici non segue solo ciò che il legislatore ha stabilito con le proprie regole ma, anzi, chiama in causa le norme sociali elaborate dal gruppo, o comunità, in cui gli individui trovano il proprio punto di riferimento, questo tipo di auto-regolamentazione e controllo è stato perfino ammirevole in molti casi. Si sono avute, per così dire, forme di "accrescimento ricorsivo", per cui ragionevoli aspettative di comportamento individuale hanno trovato riscontro e si sono alimentate reciprocamente, con un meccanismo che, nel corso delle pagine precedenti, si è illustrato con la formula dell'"opt in" (§§ 4.3.3.2 e 5.3).

Questo non significa, va da sé, che i problemi non siano mancati: dal punto di vista del rapporto tra impresa privata e singolo individuo, una delle maggiori difficoltà è dipesa dalla politica d'"informativa e consenso" messa a punto sin dal 1980 dall'OCSE (§ 6.3.2). Con un'idea ripresa da numerose legislazioni nazionali e internazionali, come nel caso di quella comunitaria, l'approccio sta a riassumere le condizioni di legittimità per il trattamento dei dati personali, nel senso che l'individuo deve essere adeguatamente informato tanto sulle finalità per cui i dati sono raccolti, quanto sulle modalità del trattamento e i destinatari, o le categorie dei destinatari, per i quali i dati sono trattati, al fine di dare eventualmente, su queste basi, il consenso alla raccolta e trattamento dei propri dati (§ 8.2.2). Alla prova dei fatti, però, questo meccanismo d'"informativa e consenso" si è inceppato per svariati motivi, alcuni dei quali ben noti al lettore.

In primo luogo, l'informativa dei fornitori di servizi è spesso mostruosamente prolissa e complessa: c'è chi si è perfino divertito a notare che i termini di servizio di PayPal, incluse le specifiche sul trattamento dei dati, ammontano, nella versione inglese, a 36275 parole, vale a dire più dell'Amleto di Shakespeare (30066 parole). Le cose non stanno poi tanto meglio con iTunes, la cui informativa supera la lunghezza del Macbeth, 19972 a 18110 parole (v. Parris 2012). Il risultato è che, il più delle volte, gli utenti si guardino bene dal passare giornate intere a leggere e comprendere le condizioni del servizio che viene loro offerto.

In secondo luogo, anche qualora gli utenti abbiano la pazienza di scrutare tutte

le clausole dell'accordo, difficilmente sarebbero in grado di districarsi nei tecnicismi delle formule giuridiche e con le condizioni proposte dai fornitori tramite i propri termini di servizio. Questi ultimi, in fondo, si avvalgono spesso di una nutrita schiera di avvocati, al fine proprio di non incorrere nel rigore sanzionatorio della legge, attraverso termini generali, oppure clausole specifiche, ecc.

In terzo luogo, l'approccio dell'"informativa e consenso" presuppone una parità tra le parti dell'accordo che, spesso, non solo non rispecchia ma contraddice la realtà. Sul punto si sono già espresse le Autorità europee garanti della protezione dati (WP 29), nel ricordato documento del 2009 sul "futuro della privacy" (doc. WP 168). Con le loro parole, "il consenso è una base inappropriata per il trattamento [in] molti casi in cui il consenso non può essere dato liberamente, specie quando c'è un chiaro squilibrio tra il titolare dei dati e il responsabile del trattamento (per esempio, nei rapporti di lavoro o quando i dati personali devono essere dati alle autorità pubbliche)".

In quarto luogo, l'approccio dell'"informativa e consenso" fa ricadere sui titolari dei dati personali il compito, più che oneroso, di soppesare benefici e rischi che derivano dall'accordo. Stante le nuove tecniche di aggregazione e sfruttamento dei dati, può essere anche chiaro all'individuo il beneficio immediato che gli deriva firmando la liberatoria al trattamento; ma, il più delle volte, sono del tutto imprevedibili i rischi che possono aversi nel lungo periodo.

Alla luce dei numerosi problemi cui è andato incontro il paradigma del consenso, molti hanno cominciato a suggerire di fare attenzione più ai rischi connessi all'uso dei dati personali, che alle modalità della loro raccolta tramite il consenso come base principale per il legittimo trattamento dei dati. A ciò spingerebbero non solo i vicoli ciechi in cui, nella pratica, è andato a parare l'approccio dell'"informativa e consenso"; ma, pure il progresso tecnologico con la raccolta onnipervasiva di dati per finalità di sorveglianza, con l'abbattimento dei costi di conservazione e condivisione dei dati, fino allo sviluppo di nuove tecniche per lo sfruttamento di quei dati. "Concentrarsi sull'uso dei dati personali non significa che non ci dovrebbero essere responsabilità o regolazione per la raccolta dei dati, e nemmeno che si debba abbandonare l'idea del consenso per circostanze specifiche o sensibili. Piuttosto, in molte occasioni, è probabile che un più pratico e accorto bilanciamento tra i flussi di dati preziosi e una più effettiva protezione della privacy si ottenga facendo maggior attenzione a un uso appropriato, responsabile" di quei dati (Cate e Mayer-Schönberger 2013: 5).

In fondo, spostando il baricentro del modello dal consenso ai rischi per l'uso dei dati personali, torneremmo all'ispirazione originaria della protezione, tanto in Europa, quanto negli Stati Uniti, per cui l'attenzione è incentrata "sulla valutazione del rischio nel prevenire il danno, piuttosto che sulla protezione dei diritti individuali alla privacy" (Cate e Mayer-Schönberger 2013: iv). In questo modo, sarebbe possibile concentrarsi nuovamente sul concetto di "trasparenza" sul quale si è attirata l'attenzione sin dall'inizio di questo capitolo, vale a dire su ciò che "aiuta a costruire la fiducia, nonché una maggiore consapevolezza sulle attività di trattamento dei dati da parte di coloro che ne hanno cura, consentendo che le autorità pubbliche, gli auto-regolatori dell'industria e i difensori della privacy siano informati e rafforzati" (*op. cit.*, v).

Inoltre, una rinnovata attenzione sui rischi dell'uso dei dati permetterebbe di affrontare le sfide poste dall'impiego di nuove tecniche, come ad esempio il *data min-*

*ing* (v. § 6.2.2), riducendo il ruolo che il consenso e la specificazione dello scopo o finalità del trattamento hanno al momento della raccolta (§ 8.2.1 e, ivi, figura 24). Infatti, se affrontando i temi della nuova sorveglianza, l'accento è caduto sull'uso di tecniche, come il *profiling* e il *data mining*, a fini "pubblico-protettivi" di controllo, qui, bisognerebbe pur ricordare come dai *big data* e gli strumenti di indagine analitica su quella mole sterminata di dati sia possibile estrarre informazioni più che preziose, ad esempio, nell'ambito della ricerca medica. Sulla base dell'odierno regime che fa leva sul consenso e le finalità d'uso dei dati, il più delle volte non è lecito ricavare questo valore aggiunto, come conferma il caso del riuso delle informazioni nel settore pubblico (PSI), perché spesso le nuove modalità d'uso dei dati risultano semplicemente impensabili al momento della raccolta dei dati stessi. L'impossibilità di fare un uso legittimo e finanche utile dei dati personali per mancanza di consenso sui fini del trattamento, mostrerebbe perciò una ragione ulteriore per ridimensionare il ruolo che il concetto svolge nel modello europeo della privacy, facendo attenzione invece sui rischi che derivano dall'uso, anche in parte imprevedibile, di quei dati.

È pertanto al tema dell'uso e riuso dei dati personali, che sono dedicati i seguenti paragrafi del capitolo.

## 8.4. *Uso e riuso*

Il riferimento all'uso dei dati personali è stato fin qui fatto in rapporto alle finalità o scopi del trattamento, sulla base sia del consenso dell'interessato, sia delle cinque ipotesi che rendono legittimo quel trattamento, anche senza il consenso del titolare dei dati (§ 8.2.2). Da questo punto di vista, l'analisi delle condizioni di legittimità per l'uso dei dati personali rappresenta il terzo stadio nel ciclo vitale di questa informazione: quanto s'è detto sugli osservabili e variabili delle figure 23 e 24 del presente capitolo, può essere ora approfondito con un ulteriore livello di astrazione. Si dia un'occhiata alla figura 25.

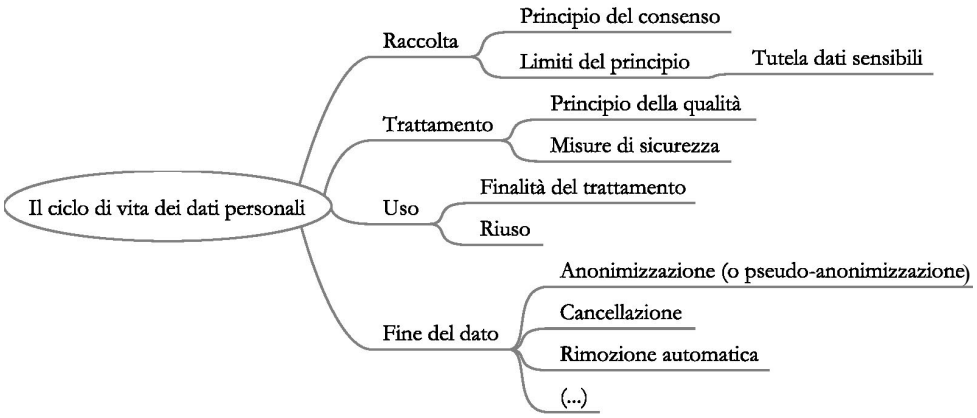


Figura 25: *Il ciclo di vita informativa del modello*

Secondo il ciclo di vita dei dati personali abbiamo, così, in primo luogo i problemi relativi alla raccolta, o caricamento immediato nel sistema informativo, dei dati personali sulla base della regola generale del consenso, per quanto essa venga temperata dalle sue eccezioni. Dopo di che, seguono le questioni della legittimità del trattamento, sia in termini di qualità (§ 8.2.1), che con le relative misure di sicurezza (§ 8.2.4), per poi passare, appunto, al tema di questo paragrafo, e cioè l'uso dei dati personali. Lasciando, per ora, da parte "la" – più che "il" – fine che può toccare al dato personale, la figura 25 mostra due variabili d'uso: quella della finalità che rende legittimo l'uso dei dati personali, di cui si è detto poco fa, e il riuso di questi stessi dati personali.

Nel primo caso, la finalità del trattamento può prevedere essa stessa il possibile riuso del dato personale: è il caso dello studente universitario che, al momento d'iscriversi al primo anno di studi, rilascia agli uffici la liberatoria per il trattamento dei suoi dati che, però, da alcuni anni prevede, con il consenso dello studente, che quei dati possano essere un giorno riutilizzati dai servizi di ricerca lavoro dello stesso ateneo.

Nel secondo caso, si pone invece il problema con cui abbiamo chiuso il paragrafo precedente, ossia come la vigente normativa sulla protezione dei dati personali ostacoli molti riusi, ragionevolmente legittimi, di quegli stessi dati. È il caso tormentato del riuso dei dati del settore pubblico, o *public sector information* (PSI), che, spesso, a proposito di dati nei registri commerciali, catasti, motorizzazione, casellari giudiziari, sistema sanitario e dati socio-economici vari, ha visto frapporsi la protezione, vera o presunta, dei dati personali, a un riutilizzo proficuo di quei medesimi dati (Pagallo e Bassi 2013). Si tenga solo presente che, nello studio predisposto per la Commissione europea nel 2011 sull'impatto economico della informazione del settore pubblico, il cosiddetto rapporto Vickery, si è stimato che i guadagni, diretti e indiretti, dovuti al riuso di quei dati, ammonterebbero a circa 140 miliardi di euro all'interno dell'Unione. Tra i metodi proposti per uscire dal vicolo cieco rappresentato dal conflitto tra le norme europee sulla protezione dati e il riuso dell'informazione nel settore pubblico, o PSI (D-2013/37/CE), pare consigliabile concentrarsi sui rischi d'uso, più che sul consenso prestato a suo tempo dagli interessati, come detto nel paragrafo precedente. In fondo, questa è anche l'idea proposta sia dal regolamento della Commissione, sia dalle autorità garanti (WP 29), allorché insistono sull'importanza di condurre perizie e stime per calcolare l'impatto che determinati usi (e riusi) dei dati personali possono avere su questi dati.

Oltre a quanto in gergo è conosciuto come *privacy impact assessment* e *data protection impact assessment*, un'ulteriore tecnica di riuso riguarda l'anonimizzazione dei dati, vale a dire la loro riduzione alla condizione di inutilizzabilità ai fini dell'identificazione di una persona fisica o "naturale" (§ 6.2.1). Come espresso dalle autorità garanti (WP 29) con l'opinione del 2 aprile 2013 (doc. WP 203), le tecniche di anonimizzazione rappresentano "la soluzione più soddisfacente per minimizzare i rischi di divulgazione involontaria" di dati personali. Questo è stato anche l'approccio della direttiva europea sui "sistemi di trasporto intelligente" (ITS) per la rete stradale e le interfacce con altri sistemi di trasporto. Secondo formula di stile, al pari della normativa D-2013/27/CE sul riuso della informazione del settore pubblico, anche il considerando 12 di D-2010/40/CE (o direttiva ITS) afferma la necessità di

salvaguardare i diritti alla protezione dei dati personali D-1995/46/CE; e, in particolare, i principi della limitazione dello scopo del trattamento e la minimizzazione dei dati raccolti. Tuttavia, continua a essere la direttiva ITS, all'articolo 10, che prevede l'anonimizzazione dei dati personali raccolti nelle banche dati dei sistemi di trasporto intelligente, al fine del riuso di quei dati.

A volte, non è nemmeno richiesto provvedere alla completa anonimizzazione dei dati ma, nei termini delle Autorità WP 29, alla "pseudo-anonimizzazione". Con l'opinione 4 del 2007 (doc. WP 136), "usare uno pseudonimo significa che è possibile risalire all'individuo, cosicché la sua identità possa essere scoperta, ma soltanto in alcune circostanze predefinite. In tali casi, benché le norme sulla protezione dei dati trovino applicazione, i rischi che corre l'individuo per il trattamento di tale informazione, solo indirettamente identificabile, saranno il più delle volte bassi. Ne segue che l'applicazione di quelle regole [per la protezione dei dati] saranno giustificatamente rese più flessibili di quanto non avvenga per il trattamento d'informazioni che rendano gli individui direttamente identificabili". Questo approccio più flessibile, suggerito fin dal 2007, è stato peraltro ripreso dalla più recente opinione del 2013, dove WP 29 afferma che "l'anonimizzazione dovrebbe essere fatta, ancor prima di rendere il dato disponibile per il riuso" e "conducendo un effettivo *data protection impact assessment* per decidere che dati possano essere resi disponibili al riuso e secondo quale livello di anonimizzazione e di aggregazione" (doc. WP 203 dell'aprile 2013).

Questa prospettiva che fa leva sui rischi d'uso, più che sul consenso, per determinare la liceità del trattamento dei dati personali, è peraltro consigliata dallo stesso riposizionamento tecnologico dell'istituto. È quanto emerso con gli esempi delle fotografie (§ 6.1.1), delle banche dati (§ 6.1.2), del Web 2.0 (§ 6.1.3); e, poi, con la tecnologia del telefono (§ 7.2.1), le cabine telefoniche (§ 7.2.2), le camere fotografiche per aerei e i satelliti (§ 7.2.4), fino ai sensori termici (§ 7.3.1), e gli smartphone (§ 7.5.2).

Alcuni presentano il nuovo scenario, facendo leva sulla de-contestualizzazione e ri-combinabilità del contenuto dei messaggi individuali (Kallinikos 2006); altri insistono sulle questioni di persistenza, replicabilità, scalabilità e rintracciabilità delle informazioni (Boyd 2010). Qui, suggerisco di cogliere, dal punto di vista del possibile rischio dell'uso di quei dati da parte dei terzi, come i dati personali sono usati e riusati, una volta immessi su internet o, in genere, nell'infosfera. L'accento non cade soltanto sulla necessità di concentrarsi sui rischi del riuso sottolineati dalle Autorità garanti (WP 29), o di quelli derivanti dalle nuove tecniche e usi segnalati da Kallinikos (2006) e Boyd (2010). Molti dei riusi cui sono sottoposti i dati personali hanno infatti a che fare con le aspettative, interessi o veri e propri diritti, che altri individui vantano su quegli stessi dati. Basti pensare al diritto di parola, di libertà d'espressione, cronaca o informazione, ecc. Si tratta in fondo di un tema classico della materia, a proposito del bilanciamento di un diritto con altri diritti e libertà fondamentali. Rifacendoci alla giurisprudenza della Corte di Lussemburgo, ne abbiamo fin qui parlato a proposito della tutela dei diritti di proprietà intellettuale, nel bilanciamento, appunto, con la tutela dei dati personali (§ 5.4.3). Inoltre, abbiamo poco fa ricordato il reticolo di direttive "PSI" (D-2013/27/CE), "ITS" (D-2010/40/CE), e quella per la protezione dati, dove l'esigenza è di bilanciare quest'ultimo diritto con il di-

ritto alla trasparenza amministrativa, all'informazione, all'efficienza dei trasporti o alla libertà di parola. Si tratta ora di comprendere come il modello europeo abbia inteso governare questa fase della vita informativa dei dati personali. La figura 26 illustra i nuovi osservabili dell'indagine:

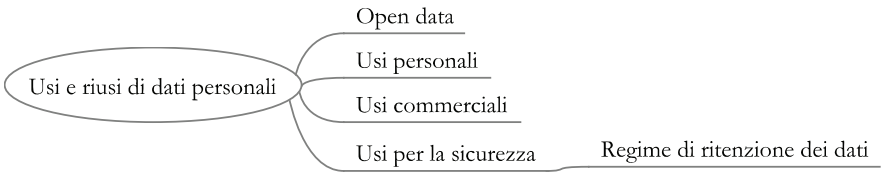


Figura 26: *Tra apertura e ritenzione dei dati personali*

Da quest'ulteriore punto di vista, conviene concentrare l'attenzione, innanzitutto, sulla criticità del ciclo degli usi e riusi di dati, sulla base di un paradigma apparentemente opposto a quello della privacy, ossia, quello dell'"apertura dei dati" o *open data* (§ 8.4.1).

In secondo luogo, sarà bene chiarire nel nuovo contesto della quarta rivoluzione cosa debba intendersi per "usi personali" (§ 8.4.2).

In terzo luogo, potremo capire come il modello europeo sul riuso ne disciplini gli "usi commerciali" (§ 8.4.3).

Infine, il riferimento andrà alla disciplina sugli usi dei dati personali ai fini della sicurezza in Europa (§ 8.4.4), con particolare riguardo al regime della ritenzione dei dati medesimi.

In questo modo, saremo pronti ad affrontare le questioni di responsabilità che si pongono per ciascun uso.

### 8.4.1. *Dati aperti*

Il movimento dell'apertura dei dati, come trasparenza nelle istituzioni (e della società), vanta illustri precedenti. Basti solo pensare al titolo dell'opera che, nel 1945, uno dei più illustri filosofi del Novecento, Karl Popper (1902-1994), dava alle stampe: *La società aperta e i suoi nemici*. Nella tradizione costituzionale dei moderni, abbiamo visto due classi di principi che richiedono siffatta apertura: sono i principi fondamentali dell'ordinamento che richiedono per se stessi informazione, come nel caso del diritto di formarsi un'opinione (§ 5.3.3.1); e i principi che viceversa necessitano che l'informazione sia divulgata, come avviene con il diritto di cronaca o la libertà di parola (§ 7.1). Da questo punto di vista è comprensibile che, parlando di apertura dei dati, l'attenzione ricada sui fattori dai quali tale apertura dipende, come la disponibilità dell'informazione o le condizioni della sua accessibilità che, spesso, sono disciplinate dai singoli ordinamenti nazionali con apposite leggi sulla libertà di informazione.

Invece, la particolarità della tutela dei dati personali consiste precisamente nel restringere questi flussi informativi, al fine di proteggere le persone dai possibili danni. Ciò ha dato a molti l'impressione che la disciplina dei dati personali non pos-

sa che opporsi alla stessa apertura, o riuso, dei dati, secondo una logica del tutto o niente. In realtà, sebbene non siano mancati i casi in cui la protezione della privacy non è che una semplice scusa del funzionario per non adempiere al proprio compito, bisogna avvertire che le due sfere finiscono spesso per sostenersi a vicenda. Si pensi alla trasparenza cui si ispirano sia la normativa sulla tutela dei dati, sia i sostenitori dei dati aperti: in molti casi, come nella trasparenza e apertura dei dati detenuti dall'amministrazione pubblica, tutela della privacy ed efficienza delle istituzioni possono andare a braccetto.

In secondo luogo, dal punto di vista concettuale, la privacy, a sua volta, non è da intendersi come un gioco a somma zero di esclusione, limitazione o controllo (figura 18 di § 6); bensì, va concepita in rapporto a un accesso ristretto e a un controllo limitato. Come abbiamo già visto, le scelte personali giocano un ruolo determinante nel modulare diversi livelli di accesso e di controllo, dipendendo dal contesto e dalle sue circostanze (§§ 8.2.2 e 8.3.1). Inoltre, fin dall'origine, tanto il diritto alla privacy, quanto il diritto alla protezione dei dati, non sono stati concepiti come un gioco a somma zero, per il buon motivo che essi devono essere bilanciati tanto con le esigenze della sicurezza pubblica e nazionale, quanto con gli ulteriori diritti e libertà che gli individui hanno nell'ordinamento.

In terzo luogo, abbiamo anche riferito come il tradizionale bilanciamento tra i vari diritti e interessi tutelati dall'ordinamento, sia stato aggiornato tecnologicamente dai nuovi strumenti per l'anonimizzazione o, anche, pseudo-anonimizzazione dei dati (§ 8.4). Sebbene non siano mancate critiche, nel senso che sarebbe "stato dimostrato quanto spesso si possa ri-identificare o de-anonimizzare un individuo nascosto in dati anonimizzati con facilità strabiliante" (Ohm 2009), molto spesso sono stati sviluppati metodi efficaci per contemperare le opposte esigenze all'apertura e controllo sui dati (Pagallo e Bassi 2013: 186-187), con i motivi di ciò che abbiamo imparato a conoscere come "privacy tramite design" (§§ 5.4.3 e 6.2.4).

Queste considerazioni, naturalmente, non intendono negare che non esistano problemi; e, anzi, si tratta ora di affrontarli analiticamente, a partire dal più elementare degli usi, ossia quello personale.

### 8.4.2. *Usi personali*

A partire dalla prima direttiva comunitaria del 1995, il legislatore ha introdotto un'esenzione per le attività di trattamento dei dati, svolte "da una persona naturale nel corso di un'attività puramente personale e domestica" (articolo 3(2) di quella direttiva). Sia pure con qualche variazione restrittiva, la regola riappare anche con la proposta del nuovo regolamento della materia, presentata dalla Commissione europea all'inizio del 2012, per cui le norme di detto regolamento non si applicano ai dati personali trattati "da una persona naturale senza alcun interesse di profitto nel corso della sua attività esclusivamente personale o domestica" (articolo 2(d) del nuovo regolamento).

Nonostante l'apparente chiarezza dell'esenzione, l'incalzare dell'innovazione tecnologica può tuttavia rendere complicato stabilire la natura domestica o personale di quell'attività, tant'è che il legislatore europeo ha pensato bene di restringere il raggio della esenzione, specificando che detta attività non debba avere mire di pro-

fitto e, inoltre, debba essere personale in forma "esclusiva". Fin dal capitolo terzo (§ 3.4.1), abbiamo in fondo riferito come possa essere difficile stabilire la natura domestica o pubblica, privata o sociale, delle informazioni e dei dati che gli individui caricano in rete: se, nel caso *Lindqvist* discusso a proposito del rapporto tra gubernaculum e iurisdictio, abbiamo visto come la Corte di giustizia abbia deciso che le informazioni caricate dagli individui sulle pagine web non comportino di per sé una trasmissione di quei dati a paesi fuori dall'Unione, un altro dei problemi discussi dalla corte in quel caso era se, nel caricare quei dati sulla propria pagina web, la signora Lindqvist non li stesse in realtà trattando per uso personale o domestico. La questione che la corte ha risolto con formula negativa nel 2003, rischia tuttavia di ripresentarsi a breve sotto nuove sembianze, non appena si presti attenzione all'uso domestico di applicazioni robotiche connesse a internet: nel trattenere rapporti, entro le proprie mura domestiche, con un agente intelligente artificiale, come una badante robotica o un segretario elettronico tutto fare, fino a che punto tale attività di trattamento dati è domestica? Come intendere la nuova formula del legislatore circa l'interesse personale di trarne profitto?

Una seconda classe di problemi particolarmente delicati riguarda l'uso dei dati personali di terzi che un individuo fa in proprio: si tratta dell'esperienza quotidiana dei lettori, nell'atto di caricare sulle piattaforme sociali foto, video o altri materiali relativi ai propri amici, o semplici conoscenti. Al riguardo, è oltremodo significativo che il gruppo europeo delle autorità garanti (WP 29) se ne sia occupato appositamente con un'opinione del 12 giugno 2009, sulle reti sociali sul web (doc. WP 163). In quella occasione, le autorità affermavano che i fornitori di detti servizi (*social network services*), avrebbero dovuto avvertire gli utenti "che le foto o le informazioni su altri individui possono essere caricate soltanto con il consenso di quegli individui"; sebbene le autorità garanti non si nascondessero il paradosso al quale la normativa, tuttora vigente, avrebbe condotto, qualora i fornitori di tali servizi (SNS) si fossero attivati a fini di garanzia e tutela. Con le parole dell'Opinione, "se anche l'SNS avesse i mezzi per contattare chi non fa parte [della piattaforma sociale], per informarlo sull'esistenza di dati personali che lo riguardano, un possibile invito tramite email di unirsi alla piattaforma per visionare i propri dati personali finirebbe per violare il divieto stabilito dall'articolo 13.4 della direttiva sulla privacy elettronica [D-2002/58/CE], sull'invio di messaggi elettronici non richiesti a fini diretti commerciali" (WP 163).

Un'ulteriore preoccupazione delle autorità garanti riguardava poi l'intreccio, spesso inestricabile, tra il trattamento dei dati personali a uso proprio degli utenti delle reti o piattaforme sociali, e il trattamento che di quei dati fanno sia i fornitori di servizi (ISP), sia, più in particolar modo, di *social networking* (SNS). Ancora una volta riprendendo le parole del gruppo WP 29, "i fornitori SNS offrono piattaforme per la comunicazione in rete che consentono agli individui di pubblicare e scambiare informazioni con altri utenti. Questi fornitori di servizi sono responsabili dei dati, dal momento che stabiliscono tanto le finalità quanto i mezzi per il trattamento di detta informazione". Ma allora, ferma restando la responsabilità personale per l'uso e il trattamento che uno fa dei dati personali di altri individui, mandando messaggi su Twitter o WhatsApp, caricando video su YouTube o postando foto su Instagram, ciò significa che l'uso personale di tali informazioni s'intreccia indissolubilmente con l'uso commerciale di quei dati da parte dei fornitori SNS?

### 8.4.3. *Usi commerciali*

Ci sono due tipi principali di usi che le imprese commerciali fanno dei dati personali. Nella prima categoria vanno i trattamenti dei dati che riguardano il rapporto tra impresa privata e singolo individuo, sulla base generalmente di un accordo. Si tratta degli obblighi che l'impresa ha di assicurare la qualità del trattamento dati, su cui ci siamo soffermati nel corso delle pagine precedenti (§§ 8.2.1 e seguenti).

C'è poi il trattamento che le imprese fanno dei dati caricati direttamente dagli utenti attraverso le piattaforme e le reti sociali sul web: su un altro fronte (§ 6.3.1), sono emerse le disavventure giudiziarie di una società, come Google, che avrebbe consentito ad alcuni ragazzi di caricare sulla sua piattaforma per video, le immagini di un fanciullo autistico nell'atto di essere molestato e sbeffeggiato dai compagni di scuola. Nel corso degli ultimi anni, la responsabilità delle imprese private, quali i fornitori di servizi per internet (ISP), o di servizi per il social network (SNS), è stata uno dei temi più tormentati dell'evoluzione tecnologica in ambito giuridico, sia perché quelle imprese controllano il flusso di buona parte dell'informazione che circola in rete, sia perché esse rappresentano lo snodo attraverso cui gli individui comunicano e scambiano dati personali su terzi. Si è ricordato come la rete di ISP e SNS, in Cina, sia sotto lo stretto controllo del governo; mentre in Europa, nel dicembre 2010, la Commissione è giunta a minacciare d'imporre agli ISP l'obbligo di installare per i propri servizi "un sistema di filtraggio per tutte le comunicazioni elettroniche", specialmente per le applicazioni P2P (v. infatti § 5.2.3). Sono quelle misure normative che individuano negli ISP e SNS una sorta di sceriffo della rete, che ritroviamo nell'impostazione della legge britannica *Digital Economy Act*, del 2010, su cui abbiamo già discusso (§ 5.4.3).

Senza, però, entrare ancora nel merito della questione circa gli ISP "sceriffi della rete", occorre notare come la questione si intrecci a un altro settore dell'ordinamento – rispetto alla tutela dei dati personali – e, cioè, le norme della direttiva 2000/31/CE sul commercio elettronico (disposizioni recepite in Italia con il D.L. 70 del 2003). Sono venuto, nel corso degli anni, insistendo più volte sull'intreccio tra le due normative (Pagallo 2008; 2009; 2011; ecc.); ed è, dunque, quasi con piacere che posso salutare la nuova formulazione dell'articolo 2 del regolamento presentato dalla Commissione nel 2012. Al secondo punto dell'articolo sono stabilite le eccezioni, a noi ben note, all'applicabilità delle norme generali in tema di protezione dati, ossia, "nel corso di un'attività che fuoriesce dalle competenze del diritto dell'Unione, con particolare riguardo alla sicurezza nazionale" e affini, oltre ai casi di usi personali di cui al paragrafo precedente. Al terzo punto dell'articolo 3 del regolamento, novità assoluta dal punto di vista lessicale, si legge ora che "questo Regolamento non dovrà in alcun modo compromettere l'applicazione della Direttiva 2000/31/CE, in particolare le norme per la responsabilità degli intermediari di forniture di servizio ai sensi degli articoli, da 12 a 15, di tale direttiva".

Su queste basi, parlando di usi commerciali dei dati personali, bisogna per ciò distinguere tre diversi fornitori di servizi nel settore del commercio elettronico e, cioè, a seconda che i servizi riguardino la mera trasmissione dell'informazione (articolo 12), la memoria informatica o *cache* (articolo 13), oppure ospitino l'informazione degli utenti (articolo 14). Il risultato è che, a seconda del tipo di servizio, inerente

alla trasmissione o distribuzione di informazioni in rete, muta anche il regime di responsabilità che gli ISP hanno:

i) i trasmettitori d'informazione, come le compagnie telefoniche, sono immuni da responsabilità, a condizione che non diano inizio alla trasmissione, oppure selezionino i destinatari della trasmissione, o modifichino la sostanza dell'informazione contenuta nel dato trasmesso (art. 12);

ii) nel caso della memorizzazione temporanea dell'informazione, il fornitore del servizio non è responsabile se adempie alle condizioni e norme per accedere o aggiornare l'informazione, e "non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni" (art. 13(d));

iii) nel caso che il prestatore dei servizi "ospiti" dati e informazioni dei propri utenti, come nel ricordato caso di Google, l'immunità di quest'ultimo dipende dal fatto che "il fornitore non abbia conoscenza attuale dell'attività o informazione illecita"; e, venutone a conoscenza, "agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso" (art. 14.1(b)).

Questi tre livelli di responsabilità sugli usi commerciali, vanno poi completati con una clausola generale d'immunità, quella dell'articolo 15 della direttiva sull'e-commerce:

iv) "Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite" (art. 15.1).

Un'analoga forma per accertare le responsabilità per l'uso commerciale dei dati vige, ad esempio, negli Stati Uniti, dove gli ISP vengono classificati come trasmettitori di comunicazione elettronica, conservatori di memoria e ospiti di contenuti immessi dagli utenti, cui vanno aggiunti i fornitori di strumenti di localizzazione (*information-location tools*) e i motori di ricerca (v. 17 U.S.C. § 512). Queste clausole hanno fin qui consentito una robusta e sana crescita della rete sin dall'anno della loro approvazione, vale a dire il 1998 per il *Digital Millenium Copyright Act* (DMCA) nordamericano, con le sue clausole d'immunità come "porto libero" o *safe harbour*, e il 2000 per la direttiva comunitaria sul commercio elettronico con il principio generale dell'articolo 15. Nel quadro generale di queste norme e principi del sistema, vanno per ciò affrontate le questioni sugli usi commerciali dei dati personali e, cioè, a seconda dei diversi tipi e livelli di controllo che gli ISP hanno sull'informazione che viene trasmessa o condivisa attraverso i propri servizi. Le responsabilità che poi ne conseguono, dipendono proprio da questo diverso tipo di rapporto tra imprese private e utenti.

### 8.4.4. *Usi per la sicurezza*

L'ultimo osservabile della figura 26 riguarda una nostra vecchia conoscenza: gli usi che dei dati personali si fanno ai fini della sicurezza. Se ne è parlato in questo capitolo, sia in rapporto al canonico tema della sicurezza nazionale, o pubblica, in

relazione al principio della sovranità degli stati membri dell'Unione (§ 8.1.1); sia a proposito delle misure di sicurezza tra privati, nel duplice senso di *safety* e *security* (§ 8.2.4). Spesso, però, queste due sfere s'intrecciano, come si è cominciato ad appurare nel capitolo sesto, considerando la privacy ai tempi della "guerra al terrore" (§ 6.2.1), con la società della nuova sorveglianza (§ 6.2.2), e la presunta morte della privacy (§ 6.2.3). Per approfondire l'intreccio di usi pubblici e privati dei dati ai fini della sicurezza, torna qui utile tornare agli albori della guerra al terrore. Quando le autorità americane cominciarono ad adottare i primi provvedimenti, all'indomani dell'attacco alle Torri Gemelle, non sorprende che, per la natura degli attacchi, alcune delle misure fossero specificamente rivolte al controllo e la sicurezza nella rete dei trasporti aerei.

Sin dal giugno 2002, sarebbe sorta una controversia tra Stati Uniti e Unione europea: a parere della Commissione, le misure di sicurezza predisposte oltreoceano, sebbene pienamente condivisibili, avrebbero potuto entrare in conflitto con le norme comunitarie a tutela e protezione dei dati personali. In particolare, il governo americano minacciava pesanti multe e il blocco dei voli da e per gli USA, ai danni delle compagnie aeree che non avessero messo a disposizione del dipartimento per la sicurezza di quel paese, i dati personali dei passeggeri di ogni volo. Senza entrare nel merito di una questione che, alla fine, si sarebbe risolta con una serie di accordi internazionali tra USA e Unione europea, nota come PNR (*Passenger Name Records*), basti dire che la novità della controversia dipendeva dal fatto che, sistematicamente, l'uso commerciale dei dati si era tramutato nell'impiego di quei dati ai fini della sicurezza. Nella lite che vide opporsi il Parlamento europeo alla Commissione e al Consiglio davanti alla Corte di Lussemburgo nel 2005, questa era proprio l'opinione dell'avvocato generale nel documento presentato il 22 novembre: "la presente causa concerne praticamente un nuovo insieme di problemi, relativo all'uso di dati commerciali per garantire l'applicazione della legge" (§ 139 dell'opinione).

Questo nuovo insieme di problemi, per dirla con l'avvocato generale Philippe Léger, reclama la distinzione di quattro scenari diversi: nel primo, sono le agenzie di sicurezza nazionale che provvedono a setacciare dati e informazioni aperte al pubblico, e per lo più immesse dagli stessi utenti nella rete, con le più moderne tecniche di *data mining* o programmi informatici per il riconoscimento facciale. Spesso le persone non hanno la benché minima idea della mole d'informazioni personali disseminate volontariamente nella rete che, tuttavia, se oculatamente ricomposte e messe assieme, danno un quadro preciso e completo di quell'individuo. È per questo motivo che lavorando, dal 2012 al 2014, come membro del comitato etico di garanzia per un progetto europeo volto alla costruzione di una piattaforma multimediale di sorveglianza su internet, sotto l'egida della Commissione europea e in collaborazione con Europol, ho suggerito, con gli altri componenti del comitato, che questo tipo d'indagine, solo all'apparenza innocuo, fosse in realtà riservato alle ricerche sugli individui indiziati di "reati gravi".

Il secondo scenario prevede i doveri che le imprese private, raccogliendo dati personali per usi commerciali, hanno nei confronti delle autorità pubbliche. La clausola generale d'immunità di cui all'articolo 15.1 della direttiva comunitaria sul commercio elettronico, va infatti integrata con il dovere di collaborazione in capo agli ISP. Come recita l'articolo 15.2, "gli Stati membri possono stabilire che i prestatori

di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi, o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati".

Il terzo scenario è quello già visto con gli accordi PNR tra USA ed Europa, per cui classi di dati personali, come quelle dei passeggeri del trasporto aereo, sono in pari tempo processate sia al fine d'uso commerciale, sia allo scopo di garantire la sicurezza nazionale.

Infine, l'ultimo scenario concerne gli obblighi di ritenzione o conservazione dei dati da parte delle imprese private, che abbiamo introdotto nel capitolo sesto (§ 6.2.2). Si tratta della "conservazione di dati di traffico per altre finalità", rispetto a ciò che è disciplinato in via ordinaria dalla legge, stabilita dall'articolo 132 del codice della privacy italiano, che, a sua volta, riconduce all'articolo 15 della direttiva 58 del 2002. Le misure ivi prese, con l'ampio margine discrezionale lasciato agli stati membri, hanno destato fin dall'inizio preoccupazioni e critiche, stante l'obbligo di conservazione indiscriminata dei dati personali, a carico degli ISP e per lunghi periodi di tempo. I timori sono stati poi confermati dalla successiva direttiva 24 del 2006, a pieno regime dal 2009, che aveva come oggetto principale gli obblighi dei fornitori di servizi nel campo della comunicazione elettronica accessibile al pubblico, di conservare determinati dati da essi generati, o trattati "allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale" (articolo 1.1 della direttiva).

Da un lato, i dati da conservare, riguardavano il traffico, l'ubicazione delle persone sia fisiche sia giuridiche, e quelli necessari per identificare l'abbonato o l'utente registrato (articolo 1.2 che, tuttavia, faceva salvo il contenuto delle comunicazioni elettroniche e le informazioni consultate utilizzando una rete di comunicazione elettronica). D'altro canto, era stabilito l'obbligo di conservare i dati (art. 3), con le modalità di accesso (art. 4), le categorie dei dati da conservare (art. 5), il periodo di conservazione dei dati (art. 6), la loro protezione, sicurezza (art. 7), e archiviazione (art. 8), i nuovi compiti delle autorità di controllo (art. 9), nonché gli accorgimenti statistici (art. 10) in vista di misure future (art. 12 e 14).

Senza entrare nel dettaglio della normativa, nonché del crescendo di critiche contro la stessa (v. Pagallo 2008: 143), è ancora una volta intervenuta, a garanzia dei diritti in gioco, la sfera della iurisdictio. A partire dal 2009, infatti, si sono pronunciate numerose corti costituzionali europee; mentre, nel 2014, è stato il turno della Corte di Lussemburgo. Nel prossimo paragrafo, il doppio registro, nazionale e comunitario, di queste sentenze servirà a chiarire ulteriormente la struttura e valori del modello europeo della protezione dei dati.

#### 8.4.4.1. *Ritenzione dei dati*

Secondo il ciclo di vita informativa dei dati personali, illustrato dalla figura 25 (§ 8.4), dopo la raccolta, trattamento e uso di quei dati, essi dovrebbero essere distrutti, cancellati o resi inutilizzabili, sia perché sono state raggiunte (o sono venute a

mancare) le ragioni del trattamento, sia perché è stato revocato il consenso dell'interessato, sia perché sono scaduti i termini del trattamento e i dati vengono rimossi in automatico dal sistema, o con provvedimento del responsabile del trattamento, ecc.

Nondimeno, a séguito degli attacchi terroristici dell'11 settembre 2001, tanto al di qua che al di là dell'Atlantico, i legislatori hanno introdotto apposite disposizioni al fine di garantire la sicurezza nazionale, allungando i termini della conservazione dei dati, nella convinzione che questi ultimi, prima o poi, sarebbero tornati utili nella cosiddetta guerra al terrore. Con l'approvazione, in Europa, della D-2006/24/CE e la successiva incorporazione della direttiva negli ordinamenti degli stati membri dell'Unione, si sono tuttavia cominciati ad avere i primi casi in cui i titolari dei dati conservati, hanno eccepito l'illegittimità delle misure di ritenzione. Più che vertere sulla fondatezza di quelle misure in rapporto alla Carta dei diritti fondamentali dell'Unione, oppure sulla compatibilità di quest'ultima con i principi supremi garantiti dalle costituzioni degli stati membri, il problema che è innanzitutto sorto, si è presentato come tipica questione di legittimità costituzionale delle leggi approvate dai parlamenti nazionali, per recepire le disposizioni comunitarie. Come tale, la questione è stata dunque discussa davanti a numerose corti costituzionali che, a partire dal 2009, nel caso della Romania, hanno provveduto a dichiarare l'illegittimità delle misure di ritenzione. Altre corti, nel 2011, hanno seguìto l'orientamento, come nel caso di Cipro e della Repubblica Ceca, mentre altri paesi, come la Svezia, si sono guardati bene dal recepire la direttiva in quanto tale.

In questa sede, è sufficiente concentrarsi sul giudizio espresso da una corte a noi nota, il Tribunale costituzionale tedesco (§§ 3.3, 4.3.2 e 8.1.3). Il 2 marzo 2010, i giudici di Karlsruhe hanno infatti dichiarato l'illegittimità delle norme con cui il legislatore nazionale aveva recepito le disposizioni della direttiva comunitaria 24 del 2006. In particolare, il Tribunale ha sentenziato l'incostituzionalità del *Telekommunikationsgesetz* (§§ 113a e b del TKG), e del codice di procedura penale (§ 100g), per la parte che consentiva la ritenzione dei dati ai sensi del § 113a TKG, perché in contrasto con l'articolo 10.1 della Legge fondamentale tedesca che tutela la segretezza nell'uso delle telecomunicazioni. Significativamente, la corte non si è rifatta alla sua dottrina sul principio di auto-determinazione informativa. Piuttosto, essa ha preso di mira la possibilità di conservare dati sul traffico telefonico o elettronico in modo indiscriminato, con la violazione del principio di proporzionalità tra i dati raccolti e le finalità perseguite dalla legge, che sollevano ulteriori problemi di sicurezza dei dati e di trasparenza circa la trasmissione dei dati medesimi.

Nel primo punto delle motivazioni della sentenza, la Corte si è tuttavia preoccupata di sottolineare i motivi per cui non si è trattato di dirimere il problema della "competenza della competenza", quasi a rinverdire antichi scontri tra Lussemburgo e Karlsruhe. Piuttosto, a giudizio del tribunale, l'oggetto della lite avrebbe riguardato il margine di discrezionalità con cui il legislatore tedesco ha tradotto nel proprio ordinamento la direttiva di Bruxelles, e la compatibilità delle decisioni del legislatore tedesco con i principi della costituzione di quel paese. Con le parole del Tribunale, "un ricorso alla Corte europea di giustizia è fuori questione, dal momento che la potenziale supremazia del diritto comunitario non rileva in questo caso. La validità della direttiva 2006/24/CE e la supremazia del diritto comunitario sui diritti fondamentali tedeschi che ne discenderebbe come conseguenza, non sono rilevanti per

la decisione. I contenuti della direttiva danno alla Repubblica federale tedesca ampia discrezione. Le due disposizioni sono essenzialmente limitate all'obbligo di conservazione [dei dati] e al suo raggio di applicazione, e non disciplinano l'accesso ai dati o all'uso dei dati da parte delle autorità degli Stati membri. Con questi contenuti, la direttiva può essere implementata nell'ordinamento tedesco senza violare i diritti fondamentali della Legge basica. La Costituzione non proibisce tale ritenzione [dei dati] sotto ogni circostanza".

Quattro anni dopo, l'8 aprile 2014, la Corte di Lussemburgo è intervenuta a sua volta sul punto, dichiarando l'invalidità della direttiva sul piano della legalità comunitaria, avendo "ecceduto i limiti imposti dal rispetto del principio di proporzionalità, alla luce degli articoli 7, 8 e 52(1) della Carta" europea dei diritti fondamentali (§ 69 di C-293/12 e 594/12). Infatti, come ammette la corte, è evidente "che la lotta contro il terrorismo internazionale per mantenere la pace e la sicurezza internazionali costituisce un obiettivo d'interesse generale […] Del pari, ciò è vero anche per la lotta contro i crimini gravi al fine di garantire la sicurezza pubblica […] Inoltre, bisognerebbe notare a questo proposito che l'articolo 6 della Carta stabilisce il diritto di ogni persona non soltanto alla libertà, ma pure alla sicurezza" (§ 42 della decisione). Ma, prosegue la corte, la piena legittimità dei fini perseguiti dalla direttiva non ne giustifica affatto i mezzi: da un lato, il combinato disposto degli articoli 3 e 5(1) della direttiva sulla ritenzione dei dati (v. sopra § 8.4.4), riguarda "la ritenzione dei dati di tutto il traffico riguardante la telefonia fissa e mobile, l'accesso a internet, le email e le telefonate in rete", per cui si "applica a tutti i mezzi della comunicazione elettronica, il cui uso è oltremodo diffuso e d'importanza crescente per la vita quotidiana delle persone […] Essa per ciò comporta un'interferenza con i diritti fondamentali di praticamente tutta la popolazione europea" (*op. cit.*, § 56). D'altra parte, "la direttiva 2006/24 non fissa alcun criterio oggettivo con il quale il numero delle persone autorizzate all'accesso e conseguente uso dei dati ritenuti sia limitato a quanto strettamente necessario alla luce dell'obiettivo perseguito. Soprattutto, l'accesso ai dati ritenuti da parte delle autorità nazionali competenti, non è fatto dipendere dal controllo preventivo di una corte o di un'autorità indipendente amministrativa, le cui decisioni possano limitare l'accesso ai dati e il loro uso a quanto strettamente necessario ai fini dell'ottenimento dei risultati perseguiti […] Del pari, essa [la direttiva] non fissa alcuna specifica obbligazione per gli Stati membri di stabilire detti limiti" (*op. cit.*, § 62). Da queste considerazioni, e citando a più riprese, in via analogica, i precedenti della Corte europea dei diritti umani di Strasburgo sul principio di proporzionalità (*op. cit.*, §§ 47, 54, 55, ecc.), ne consegue, a giudizio della Corte di Lussemburgo, che la direttiva 24 del 2006 è invalida perché in contrasto con le norme sovraordinate del sistema. Mentre, nel caso dei tribunali costituzionali tedesco, romeno, ceco, ecc., si è trattato dell'illegittimità nazionale delle norme con cui i legislatori di ciascun paese, nell'ambito della loro discrezionalità, hanno recepito la direttiva 24, nel caso della Corte di giustizia, invece, si è trattato dell'illegittimità comunitaria di una normativa contrastante con i principi sanciti dalla Carta dei diritti fondamentali.

All'atto pratico, naturalmente, il Consiglio e Parlamento europei, tenendo conto delle indicazioni dei giudici di Lussemburgo, potranno, se lo riterranno opportuno, legiferare nuovamente in materia. Nondimeno, non si tratterà di un intervento di

per sé necessario per colmare un vuoto normativo, dato che la direttiva 24 si poneva pur sempre come disciplina speciale, nel quadro delle regole predisposte dalla 46 del 1995 e, in prospettiva, dal nuovo regolamento sulla protezione dei dati, di cui parleremo nel prossimo capitolo. Sul piano teorico, tuttavia, è importante segnalare come la funzione nomofilattica della Corte riporti per questo verso alle considerazioni precedentemente svolte sia a proposito del ruolo della corte come organo di chiusura del sistema (§ 3.2.2), sia sui limiti di questa funzione (§ 8.1.1), sia in rapporto alle esagerazioni dei teorici della morte della privacy (§ 6.2.3).

Piuttosto d'insistere su quanto fin qui detto, conviene però completare la nostra analisi con l'ultimo tema fondamentale del regime di trattamento e tutela dei dati personali, quello cioè della responsabilità. Che ne è, infatti, nel caso in cui, nonostante la piena congruità della normativa, siano violati i diritti di un individuo?

## 8.5. *Responsabilità*

Secondo una prima accezione, possiamo definire la nozione di responsabilità come il rispondere, a sé o agli altri, delle proprie azioni o omissioni, così come di quelle poste in essere da altre persone, di cui abbiamo, appunto, la responsabilità.

Si tratta di una accezione sufficientemente ampia del concetto, che permette di comprendere ipotesi di responsabilità morale e politica, come nel caso, già emerso, del giuspositivismo di Hobbes (§ 2.1.2.1); e, prima ancora, di Bodin (§ 4.2.1). Sebbene il sovrano tratteggiato da questi due autori fosse sciolto dalle leggi, ossia *legibus solutus*, tanto Bodin, quanto Hobbes, si preoccupavano di spiegare che i poteri del sovrano sono in realtà limitati dalla propria coscienza davanti a Dio. È soltanto con la crisi del modello di Westfalia (§ 4.2.3), e in maniera crescente a partire dalla seconda metà del secolo scorso, che i sovrani cominceranno a rispondere delle proprie decisioni innanzi alle corti di giustizia, sulla base della consueta formula di responsabilità giuridica "se A, allora B". Secondo gli intendimenti di un allievo di Leibniz, Christian Wolff (1679-1754), a poco servirebbe il plesso di diritti e obbligazioni che siamo venuti tratteggiando in queste pagine se, all'atto pratico, non dovessero seguire le sanzioni dell'ordinamento nel caso di violazione di questi stessi diritti.

In termini generali, ci sono tre modi in cui gli individui possono confrontarsi con le clausole e condizioni di responsabilità giuridica. Con l'ultima figura del capitolo (n. 27), il riferimento va alle ipotesi di responsabilità oggettiva, immunità e responsabilità che, per colpa o dolo, dipendono dalle circostanze del caso:


Figura 27: *Tre vie alla responsabilità giuridica*

Sotto il primo osservabile della responsabilità oggettiva, gli individui sono sempre e comunque ritenuti responsabili per le azioni e omissioni, proprie o altrui, a prescindere che il comportamento concretamente tenuto dal soggetto sia censurabile dal punto di vista morale. Si pensi alla responsabilità dei datori di lavoro per gli illeciti dei dipendenti, dei padroni di animali per le malefatte di questi ultimi (salvo caso fortuito), o dei genitori per il comportamento dei figli (salvo forza maggiore). Escluse a priori tentazioni totalitarie, la ragione del principio di stretta responsabilità nasce da svariate esigenze sociali, che possono essere riassunte con il fine di distribuire i rischi dell'interazione tra gli individui. Nell'ambito della tradizione anglo-americana dell'"analisi economica del diritto", questa distribuzione del rischio è sovente intesa come un bilanciamento tra i danni che un certo atto arreca alla vittima, e i costi che il danneggiante avrebbe per non compiere quell'atto (Posner 1973). In questa sede, è sufficiente fare attenzione al tipico caso di responsabilità oggettiva per i direttori di testate giornalistiche e proprietari, o editori, di una pubblicazione a stampa; per cui, in Italia, avremmo sempre responsabilità ai sensi dell'articolo 11 della legge 47 del 1948. La ragione dipende dalla tradizionale architettura "uno-a-molti" di questi mezzi di comunicazione.

D'altra parte, l'ordinamento può prevedere una condizione di assoluta esenzione di responsabilità, nonostante il comportamento possa anche essere censurabile, sotto altro aspetto, in sede morale. Le ragioni dell'immunità sono le più varie: in sede penale, sulla scia di Hobbes e l'antica massima, per cui tutto ciò che non è proibito è lecito, si tratta del principio di legalità riassumibile con il brocardo latino "nessun delitto e nessuna pena, senza legge" (v. § 2.1.2.1); formalmente recepito dalla Convenzione europea dei diritti umani del 1950. Come recita l'articolo 7.1, "nessuno può essere condannato per una azione o una omissione che, al momento in cui è stata commessa, non costituiva reato secondo il diritto interno o internazionale"[3]. Questa è la ragione per cui, di tanto in tanto e spesso per via dell'innovazione tecnologica, i legislatori sono chiamati a intervenire, aggiungendo qualche nuovo reato: per esempio, come detto nel capitolo primo (§ 1.4.2), ciò è quanto occorso fin dai primi anni novanta del secolo scorso con una nuova generazione di crimini informatici. In sede civile, il principio di esenzione di responsabilità può a sua volta dipendere sia da clausole generali – come nel caso dell'immunità che discende dal fatto che nessuno sia tenuto all'impossibile: *ad impossibilia nemo tenetur* – sia da specifiche leggi. Agli articoli 12-15 D-2000/31/CE e § 512 DMCA in America, ricordati poco fa (§ 8.4.3), è da aggiungere il § 230 del *Communications Decency Act*, stante il quale nessun prestatore di servizi in rete o intermediario su internet può essere ritenuto responsabile per i danni arrecati dagli utenti del servizio. La ragione che, in questi casi, ha suggerito di abbracciare senza dubbi di sorta il principio di esenzione di responsabilità, dipende dalla convinzione che soltanto questo principio può promuovere e garantire alcuni diritti e libertà fondamentali nell'ordinamento.

---

[3] Come sanno gli esperti, l'articolo 7 prevede un secondo punto, stante il quale "il presente articolo non ostacolerà il giudizio e la condanna di una persona colpevole di una azione o di una omissione che, al momento in cui è stata commessa, costituiva un crimine secondo i principi generali di diritto riconosciuti dalle nazioni civili". La ragione dell'inciso dipende dall'intento di comprendere anche la disciplina di casi eccezionali, come occorso ai tempi del processo di Norimberga contro i gerarchi nazisti (v. § 4.2.2).

Il terzo e ultimo osservabile della figura 27 concerne i casi in cui la responsabilità giuridica non è né esclusa né decisa a priori, ma è stabilita a posteriori sulla base delle circostanze del caso. Si tratta in fondo della classe più comune di casi previsti dagli ordinamenti e che, ora, si lega agli accordi tra privati tramite contratti, ora, rinvia alla responsabilità che discende dal dolo, o colpa, dell'agente, sia in sede penale, sia in sede extra-contrattuale e amministrativa. Nel settore della tutela e protezione dei dati personali, sono i casi già affrontati con i termini del servizio (§ 8.3.1), e della responsabilità verso terzi che sorge dall'uso e riuso dei dati personali (§§ 8.4-8.4.3).

Approfondiamo a continuazione questi temi, soffermando l'attenzione su due aspetti della responsabilità: quella "personale" (§ 8.5.1), e quella "civile" (§ 8.5.2), che condurrà, infine, al tormentato tema della responsabilità dei fornitori di servizi in rete (si v. infatti § 8.5.2.1-2).

### 8.5.1. *Responsabilità personale*

Tornano ciclicamente le lamentele e proteste di coloro i quali ritengono che la rivoluzione tecnologica abbia condotto, a ben vedere, a una specie di hobbesiano stato di natura elettronico, in cui prevale la legge del più forte, o il caos, o l'impunità delle azioni dei malintenzionati (v. Cohen-Almagor 2010).

Le ragioni, peraltro, sarebbero le più disparate: in certi casi, la mancanza di apposite leggi; a volte, la difficoltà di attuarle; in altre occasioni, infine, il senso d'irresponsabilità generato dai nuovi mezzi della comunicazione (ICT). Per anni, il lettore ricorderà come, prima di usufruire di uno spettacolo cinematografico, fosse necessario assistere alla pubblicità progresso dei detentori di diritti di proprietà intellettuale, per cui, attirando l'attenzione su un ragazzo nell'atto di scaricare illecitamente dalla rete un video o un file musicale, lo si metteva a confronto con il suo stesso diverso atteggiamento nel mondo reale, nel quale si presume che egli non avrebbe mai pensato di rubare un portafoglio, una borsetta, un disco da una macchina, ecc.

In realtà, senza che sia necessario negare l'evidenza dei problemi aperti nel mondo della rete, occorre distinguere due diversi piani dell'analisi. Da un lato, il senso d'irresponsabilità può dipendere sia dall'obiettiva difficoltà di rintracciare e identificare il comportamento dei singoli individui in rete; sia dall'opposizione tra le norme del legislatore e le norme sociali diffuse nel nuovo ambiente, secondo un tema che siamo venuti sviluppando lungo le pagine di questo volume (§§ 1.4.3, 5.4.2 e 6.3.3).

D'altro canto, è indispensabile differenziare la responsabilità che gli individui hanno per via dei loro accordi, dalla responsabilità verso terzi in sede penale e civile. Sul primo fronte, siamo ricondotti ai temi delle controversie che possono sorgere per via del tenore delle clausole degli accordi, oppure dei termini del servizio; ciò che può allargare la lite a tutti o a parte degli utenti di un servizio informativo, o di una piattaforma sociale (§ 6.1.3). Inoltre, la discussione può riguardare sia il significato dell'accordo raggiunto tra le parti, sia il rispetto da parte dell'impresa privata, o del fornitore del servizio, delle norme imperative stabilite dall'ordinamento. Come ripetutamente detto (§§ 6.1.2, 6.2.2, 6.3.1, ecc.), i modelli europeo e statunitense sulla tutela dei dati personali si ispirano a due approcci per molti versi antitetici: all'idea americana dell'auto-regolamentazione e dei codici di disciplina, che affida sostanzialmente alle norme sociali un ruolo di prim'ordine nella tutela dei dati per-

sonali nel settore privato, si affianca e, in certi casi, si contrappone il modello europeo che fa leva su una politica legislativa che, per lo più, addotta un approccio "dall'alto verso il basso". Nel caso Katz, abbiamo visto la Corte suprema affermare che la protezione del diritto alla privacy è "ampiamente lasciata ai singoli stati" dell'Unione[4]; invece, in Europa, il punto può essere espresso con il § 96 della decisione della Corte di giustizia nel caso Lindqvist, per cui gli stati membri dell'Unione hanno il dovere d'implementare lo standard generale di protezione stabilito dalle direttive europee (C-101/01). Ciò che è valso in questi anni in materia e, cioè, la "supremazia del diritto comunitario", a maggior ragione varrà nei prossimi anni con l'adozione del regolamento.

Molti dei problemi giuridici fin qui emersi, con l'interazione sociale in rete e la tutela dei dati personali, concernono tuttavia l'ulteriore responsabilità che gli individui hanno verso i terzi in sede penale e civile. Sul piano penale, da oltre vent'anni, i legislatori nazionali e internazionali, come nel caso della Convenzione di Budapest sui delitti informatici del novembre 2001, sono venuti apportando innovazioni in modo più o meno oculato. Il problema principale che ne discende, non sembra per ciò derivare dalla minaccia di vuoti normativi, quanto dalla difficoltà di applicare le leggi già esistenti, per tutelare i soggetti dai nuovi crimini informatici. Anche se è possibile immaginare sin d'ora una nuova generazione di reati robotici, pure in questo caso rimarrebbe aperto il nodo dell'implementazione delle nuove misure che, come detto fin dal capitolo quinto (§ 5.2.3), in rapporto ai rischi di paternalismo (§ 5.3.3), conduce alla tentazione di risolvere il problema di come implementare la legge tramite un'applicazione automatica dei suoi termini (§ 5.4). È un tema che approfondiremo nel prossimo capitolo con il principio, ripreso dal regolamento europeo, sulla "privacy tramite design".

Sul piano civile della responsabilità verso terzi, infine, le cose cambiano ancora: in questo caso, si è chiamati potenzialmente a rispondere nei confronti di qualsiasi consociato per i danni arrecati personalmente o per via delle proprie attività pericolose, dei propri impiegati, animali domestici, ecc. Rispetto alla canonica rappresentazione della responsabilità civile, occorre però avere a mente come i rapporti tra gli individui vadano di pari passo con la natura fortemente decentrata dei nuovi mezzi di comunicazione, come avviene con l'uso dei cellulari connessi a internet, per cui i casi di responsabilità civile riguardano spesso una dinamica "molti-a-molti" che, tuttavia, individua non di rado "un" mediatore privilegiato per questa dialettica policentrica. La configurazione tradizionale della responsabilità civile, sia pure allargata ai confini dell'odierna globalizzazione, va perciò integrata con la dinamica topologica delle odierne reti sociali – da internet, al P2P, al web, ecc. – che tendono a coagularsi attorno a taluni nodi chiamati "hub". Questa figura della teoria delle reti, a noi già nota (v. § 2.2.2), serve a cogliere un nuovo insieme di problemi che hanno occupato studiosi e legislatori nel corso degli ultimi anni. Si tratta di approfondire questo aspetto della responsabilità civile, nel duplice senso di una responsabilità che non è penale, e che sia all'altezza di una convivenza degna della "società civile" propria della costituzione dei moderni (§§ 3.1.1 e 3.3.1).

---

[4] Rimando alla prima nota del capitolo sesto (§ 6.3.3).

### 8.5.2. *Responsabilità civile*

Oltre alle obbligazioni che gli individui contraggono volontariamente in ragione dei propri accordi, l'ordinamento prevede un ulteriore insieme di obblighi per le relazioni extra-contrattuali che, nella tradizione di civil law, sono spesso riassunti con la formula latina del non nuocere agli altri: *alterum non laedere*. Negli ordinamenti di common law, il rinvio va analogamente alla serie di doveri che la "persona ragionevole" ha di impedire "danni prevedibili" nell'ambito del tort law (Gordley 2006). In entrambi i casi, si ha la responsabilità degli individui, o d'imprese o enti, per il danno cagionato ad altri per dolo o colpa propria, con gli ulteriori casi di stretta responsabilità di cui si è fatto cenno, a proposito della responsabilità per attività pericolose, responsabilità vicaria per gli illeciti dei propri dipendenti, responsabilità oggettiva per i danni cagionati da animali, minori, ecc.

Nel settore della tutela dei dati personali, questo regime si applica del pari per i danni che gli individui possono arrecare a terzi, contravvenendo alle norme in materia di raccolta, trattamento e uso di quei dati. Si tratta di uno scenario destinato a moltiplicarsi con l'utilizzo dei nuovi media informatici (ICT) – dalle piattaforme sociali in rete agli smartphone – per cui, come detto (§ 8.2.4), le autorità garanti europee sono intervenute, consigliando ISP e SNS di avvertire gli utenti sulla necessità di richiedere il consenso degli interessati, prima di caricare o spedire foto o altre informazioni concernenti quegli stessi soggetti. Tuttavia, proprio il ruolo svolto dalle imprese private e dai fornitori di servizi in rete ha suggerito a molti che le ipotesi di responsabilità civile non riguardino i soli individui che, avvalendosi di detti servizi, rechino danno a terzi per via del proprio comportamento doloso o colposo. In realtà, questo tipo di responsabilità andrebbe estesa anche agli stessi gestori di questi servizi: in fondo, questa era la tesi avanzata qualche anno fa da un tribunale in Italia, che riteneva "ormai acquisito all'ordinamento giuridico il principio della totale assimilazione della pubblicazione cartacea a quella diffusa in via elettronica, secondo quanto stabilito esplicitamente dall'articolo 1 della legge 62/2001" (sentenza 6127 della seconda sezione civile di Milano nel maggio 2002).

Ma, a parte il fatto che la summenzionata legge 62 equipara "il prodotto realizzato su supporto cartaceo" a quello elettronico soltanto "ai fini della presente legge" – e cioè in materia di trasparenza proprietaria, erogazione di provvidenze o intervento per lo sviluppo editoriale – si può dire che i prestatori dei servizi siano veramente assimilabili ai direttori della carta stampata? Non abbiamo forse illustrato in precedenza (§ 8.4.3), il regime d'immunità per ISP e SNS stabilito tanto dal legislatore americano, quanto da quello europeo? Non è forse la relazione "molti-a-molti", sia pure mediata da questi fornitori di servizi in rete, agli antipodi del rapporto "uno-a-molti" che giustifica l'adozione di misure di responsabilità oggettiva per gli editori e i direttori della carta stampata?

Dopo l'analisi sul ciclo vitale dei dati personali, attraverso il momento della raccolta, trattamento e responsabilità per l'uso di quelle informazioni, occorre completare il quadro sulla protezione dei dati personali, avendo a mente il ruolo cruciale che gli ISP svolgono nelle odierne società ICT-dipendenti.

### 8.5.2.1. *Il ruolo cruciale degli ISP*

Quando il Parlamento e il Consiglio approvarono, l'8 giugno 2000, la direttiva sul commercio elettronico, il legislatore europeo aveva già di fronte l'esempio del legislatore di Washington che, nel 1996, aveva sancito l'immunità dei fornitori di servizi in rete per i danni arrecati dagli utenti di quei servizi, ai sensi del § 230 del *Communications Decency Act* (CDA); misura ribadita nel 1998, con il § 512 del *Digital Millennium Copyright Act* (DMCA), sia pure nel contesto più ristretto definito dalle violazioni dei diritti d'autore o copyright. Rispetto alle clausole che il legislatore europeo avrebbe finito per dover adottare con D-2000/31/CE, due specificità dell'approccio americano vanno notate.

La prima riguarda il rapporto strumentale dell'immunità accordata agli ISP in nome della libertà di parola negli Stati Uniti (v. § 7.1). In omaggio alla tradizione costituzionale di questo paese, le corti hanno infatti interpretato il § 230 CDA quale baluardo della protezione dei prestatori di servizi contro la responsabilità per fatto altrui, poiché lo scopo è "di incoraggiare lo sviluppo senza vincoli né regole della libertà di parola su internet" [5]. In questo modo viene eliminata alla radice la possibilità di concepire la responsabilità dei provider alla stregua della responsabilità oggettiva dei direttori di giornali, con i disincentivi che seguirebbero inevitabilmente all'obbligo di controllare il materiale immesso nella rete, nei social forum, nei blog, ecc., dato che il § 230 ha per scopo di esimere i prestatori di servizi dalla responsabilità "che segue all'esercizio delle tradizionali prerogative degli editori […] nell'aver cura del materiale pubblicato" [6]. In caso contrario, non si avrebbe null'altro che "un'altra forma di intrusione del governo nella disciplina [della libertà] di parola" [7]. Dai siti in cui il contenuto è prodotto dagli stessi utenti, come YouTube o Flickr, a piattaforme sociali come MySpace, all'informazione dei consumatori in siti come Yelp, a nessuno negli Stati Uniti verrebbe in mente di chiamarli in causa per i giudizi ivi espressi dagli utenti.

L'immunità accordata dal § 230, tuttavia, non esime certo dalla responsabilità che il prestatore di servizi ha nel caso in cui esso abbia materialmente contribuito alla creazione del contenuto illecito immesso in rete o abbia violato determinate disposizioni del diritto penale federale. Una ricerca empirica sull'immunità degli intermediari dei servizi sotto la copertura del § 230 ha peraltro mostrato come la norma abbia ampiamente protetto queste imprese dalla responsabilità derivante dalle opinioni degli utenti nei nuovi media e, nondimeno, l'immunità non abbia rappresentato il "via libera" a molti degli eccessi che i critici della legge paventavano: "i giudici sono andati piuttosto a casaccio nel modo di applicare la norma" (Ardia 2010). Questo approccio, per così dire, pragmatico serve anche a chiarire la seconda peculiarità delle clausole di "porto libero" (*safe harbour*) vigenti in questo ordinamento giuridico, a confronto con il modello europeo sulla tutela dei dati personali.

---

[5] Questo il giudizio della Corte d'appello in *Batzel v. Smith*, 333 F.3d 1018, 1027-28 (nono circuito, 2003).

[6] Questa volta il giudizio è della Corte del quarto circuito in *Zeran v. America Online*, 129 F.3d 330 (1997).

[7] *Ibidem*.

Il § 512 DMCA prevede infatti, come detto (§ 8.4.3), l'esenzione di responsabilità per tutti i fornitori di connettività in internet e per la memorizzazione di informazioni, motori di ricerca e siti i cui contenuti siano prodotti dagli stessi utenti: la medesima norma contempla tuttavia un meccanismo di rimozione dei contenuti, ritenuti a torto o a ragione illeciti, che fa leva sull'auto-regolazione degli attori privati e delle forze del mercato con la procedura del *takedown notice*. In sostanza, se un ente o utente ritiene che un contenuto immesso su una piattaforma sociale, o un sito di servizi in internet, violi il proprio diritto d'autore, tale ente o utente non dovrà rivolgersi alla "pubblica autorità competente", secondo il lessico dell'articolo 15.2 D-2000/31/CE visto in precedenza (§ 8.4.4). A differenza del modello europeo, l'americano prevede che il privato si rivolga direttamente all'impresa o fornitore di servizi, affinché, specificati nei dettagli di quali contenuti su YouTube, Flickr, Instagram, ecc., si tratti (*notice)*, l'intermediario si attivi immediatamente a "buttar giù" (*takedown*), ossia, a rimuovere tali contenuti dalla informazione contenuta nei propri servizi.

Questo meccanismo, ad onor del vero, ha avuto non di rado effetti controproducenti. A richiesta dell'interessato – il presunto titolare dei diritti d'autore violati con i file audio o video caricati in rete – i prestatori di servizi provvedono infatti, spesso, a rimuovere i contenuti oggetto della controversia, ancor prima di sincerarsi della fondatezza delle lamentele. Basti pensare a quanto occorso durante la campagna presidenziale del 2008, allorché, su richiesta della CBS, Fox News, the Christian Broadcasting Network e la NBC, vennero ritirati alcuni video della campagna di Obama e del senatore McCain, caricati su YouTube. Come confermano del resto i ripetuti casi di Scientology, il rischio, talora consumato, è che il meccanismo del § 512 sia utilizzato per censurare idee e opinioni altrui, sulla base della semplice denuncia d'illecito da parte di un privato.

Le cose, però, in Europa, e sia pure per altri motivi, non sono andate poi meglio. Ai nuovi obblighi minacciati agli ISP dalla Commissione nel 2010 (§ 5.2.3); ai filtri imposti agli ISP dalla normativa britannica DEA di quello stesso anno (§ 5.4.3); alle prime disavventure di Google sul fronte dei dati personali (§§ 6.2.4 e 6.3.1); si può aggiungere come l'evoluzione della tecnologia, nel campo delle ICT, abbia indotto la iurisdictio a leggere le clausole d'immunità stabilite dagli articoli 12-15 D-2000/31/CE in maniera sempre più restrittiva. Distinguendo tra servizi "neutri" e "attivi" d'intermediazione nella società dell'informazione, si è innanzitutto sostenuto che soltanto i primi godrebbero delle clausole d'irresponsabilità previste dalla normativa. Per esempio, nella sentenza del 23 marzo 2010, nel caso *Google vs. Louis Vuitton*, ossia la nota casa di moda francese, la Corte di Lussemburgo ha affermato che "al fine di stabilire se la responsabilità di un fornitore di servizi per rintracciare informazioni possa essere limitato ai sensi dell'Articolo 14 della Direttiva 2000/31, bisogna esaminare se il ruolo svolto da quel fornitore di servizi è neutrale, nel senso che la sua condotta sia puramente tecnica, automatica e passiva, mettendo in risalto la mancata conoscenza o controllo dei dati che custodisce" (§ 114 di C-236/08). Pertanto, la responsabilità dell'ISP dipende "dai termini attuali in cui si è provveduto al servizio nella causa in discussione"; con il risultato che la Corte di giustizia dell'Unione rimandava la lite in Francia, affinché il Tribunale di Parigi accertasse "se il ruolo per ciò svolto da Google corrisponda a quanto descritto nel paragrafo 114 del presente giudizio" (§ 117 della decisione).

In alcuni casi, non è difficile comprendere come funzioni questa distinzione tra servizi neutri o attivi. Si pensi agli eventi della cosiddetta "primavera araba" e a quanto è capitato a Google nella gestione dei contenuti immessi dagli utenti su YouTube. Come dichiarato dal direttore delle "politiche pubbliche" di Google nel gennaio 2011, Robert Boorstin, "avevamo un canale su ciò che stava capitando in Egitto su YouTube e in quel canale, per tre volte, si mostravano video con maltrattamenti di prigionieri (era proprio l'inizio della sommossa). Ora, in base alle nostre regole, non è permesso di mostrare violenze su YouTube. Pertanto, rimuovemmo quel canale: tre avvertimenti e quella persona viene espulsa per causa della natura di quel video".

Fin qui, come ben si vede, YouTube non è che un intermediario nella comunicazione "molti-a-molti" tipica dell'odierna interazione in rete, per cui, come tale, esso è protetto dalle clausole d'immunità vigenti tanto negli Stati Uniti, quanto in Europa. Tuttavia, prosegue Boorstin, "a un certo momento fummo contattati da un dissidente in Egitto che stava cercando di far vedere alla gente all'estero che cosa stava esattamente capitando nel suo paese. Di qui prendemmo la decisione di rimettere i video, sebbene con due avvertimenti: 1) i titoli di ciò che erano; 2) cautela per quanto avresti guardato se minorenne". A questo punto, con i termini della Corte di giustizia, è chiaro che i servizi di Google sono diventati attivi.

Nondimeno, ferma restando la responsabilità personale di chi immette o carica informazioni in rete, o genericamente illecite, o che specificamente violano la tutela dei dati personali altrui, ci sono molti altri casi in cui può diventare particolarmente ostico separare i concetti di ciò che è neutrale o, viceversa, attivo. Lo stesso progresso tecnologico, del resto, è andato in questa direzione, dato che la funzione degli intermediari si è spesso convertita nella costruzione di arcipelaghi dorati in rete, come i servizi chiusi d'email in Facebook o il sistema dei servizi offerti da Apple, che contribuiscono alla frammentazione, o balcanizzazione, della rete. Questo processo, inoltre, è andato di pari passo con una tipica modalità secondo cui le reti crescono, ossia il fenomeno del "collegamento preferenziale" (§ 2.2.2). Basti riferire che, nel febbraio 2014, un noto e prestigioso quotidiano, *The Wall Street Journal*, pubblicava un'interessante statistica sul traffico di picco relativo ai più popolari siti web e servizi in rete: Netflix era attestata, al primo posto, con il 32%, Google seconda con il 22%, Apple terza con il 4.3%, Facebook quinta all'1.5%, Amazon settima con l'1.2%, Pandora 0.5%, Tumblr 0.4%, ecc.

Il modo in cui la natura spesso attiva di questi servizi s'intreccia con il processo della loro concentrazione, ha così dato nuova linfa alle richieste di chi ritiene che gli ISP e SNS dovrebbero assumersi le proprie responsabilità, sia sviluppando nuove forme per il controllo della condotta degli utenti, sia trattando con particolare cura i dati personali. Nell'equilibrio tra le fonti del sistema e, cioè, tra gubernaculum, iurisdictio, forze economiche e norme sociali, sarebbero infatti i pochi grandi fornitori di servizi, o intermediari in rete, a trovarsi nella miglior posizione per garantire l'ordinato svolgersi dell'interazione sociale, secondo una tesi che, sorprendendo molti, sarebbe stata accolta dalla Corte di giustizia in Lussemburgo il 13 maggio 2014, nel caso *Costeja González vs. Google* (C-131/12). In quella sede, rispetto alle liti fin qui viste con i servizi di piattaforma video della società californiana, o con le sue mappe stradali, la controversia si è spostata attorno alla disciplina dell'attività principale di questa società, vale a dire i suoi motori di ricerca, per cui, modificando sostanzial-

mente i propri orientamenti sulla natura attiva o neutra dei servizi in rete, la Corte di giustizia ha finito per ridisegnare un settore chiave del sistema giuridico europeo. Per esprimere fin d'ora il punto con la metafora del capitolo secondo (§ 2.3), se internet appare come il sistema nervoso delle odierne società complesse, or bene, i motori di ricerca vanno annoverati tra i suoi organi chiave.

### 8.5.2.2. *Motori di ricerca*

Fondata nel settembre 1998 da due giovani studenti dell'università di Stanford, Larry Page (n. 1973) e Sergey Brin (n. 1973), Google ha rivoluzionato nel giro di pochissimi anni il modo di cercare informazioni navigando in rete. Nella primavera del 2002, ne parlavo con il compianto Gene Golub (1932-2007), già preside della facoltà di Computer Science a Stanford e una volta professore di Page e Brin, con i quali stava collaborando nello sviluppo del motore di ricerca destinato a diventare, di lì a poco, il più popolare del pianeta. Golub era interessato al modo in cui utilizzavo i suoi algoritmi, specialmente quando gli avevo spiegato come l'anno precedente (2001), investigando i temi della terzietà (e quaternità) del diritto, il nuovo motore di ricerca, a differenza dei suoi rivali più accreditati, mi aveva indicato nel giro di qualche frazione di secondo il più importante contributo a me ignoto, pubblicato di recente sul tema. Ciò che, ora, sembra affatto naturale, era allora un'esperienza del tutto nuova ed entusiasmante!

Da quelle prime chiacchierate sugli algoritmi di Google ne traevo profitto anche da un punto di vista giuridico e, in fondo, già qualche anno fa (Pagallo 2008: 17), scrivevo come non fossero mancate le avvisaglie del vento che muta direzione. In molti cominciavano infatti a scorgere nuovi tipi di responsabilità per Google e, più in generale, per gli ISP, secondo i modi in cui i negozianti e i librai badano a fare andare avanti i propri affari; e, cioè, prestando attenzione alle denunce sull'illiceità o inopportunità di alcuni materiali reclamizzati o messi in vendita. "Il problema non è la neutralità della Rete, bensì se dobbiamo essere neutri rispetto a questo tipo di contenuto. Moralmente parlando […] non possiamo rimanere neutrali rispetto a discorsi così allarmanti" (Cohen-Almagor 2010).

Tradizionalmente, il regime giuridico dei motori di ricerca è stato concepito in Europa come un servizio neutro, secondo il lessico della Corte di Lussemburgo. Sebbene gli algoritmi di cui si avvalgono questi motori non siano affatto neutri – ed è, in fondo, l'ovvia ragione per cui i risultati di Google non coincidono con quelli di Yahoo o di Bing – il trattamento dei dati che ne consegue è pur sempre riferito alla mole d'informazioni che altri soggetti immettono e scambiano nella rete. Questa è stata, anzi, la circostanza più spesso contestata di recente ai motori di ricerca, che sfrutterebbero attraverso la propria opera di setaccio, filtri e collegamenti, il valore delle informazioni altrui: è il caso delle proteste degli editori di giornali, di libri, ecc. Ma, da un punto di vista giuridico, il primo problema da dover appurare è se l'opera di raccolta, estrazione, registrazione e organizzazione dei dati che vengono messi a disposizione degli utenti sotto forma di elenchi dei risultati delle loro ricerche, avviene in modo automatico tramite gli algoritmi del motore di ricerca. In quest'ultimo caso, secondo i termini della Corte di giustizia nel caso *Google vs. Louis Vuitton*, la condotta del fornitore di servizi appare "puramente tecnica, auto-

matica e passiva", dato che detto fornitore non potrebbe essere a conoscenza dei dati processati, né esercitare alcun controllo su di essi, come quando ad esempio processa 70 milioni di risultati in 0.21 secondi per rispondere alla mia richiesta di notizie sulla "CNN". Nel caso in cui, viceversa, il motore di ricerca alterasse i risultati per favorire, poniamo, i propri clienti a pagamento, va da sé che, oltre a problemi etici e di fiducia con gli utenti, il fornitore del servizio sarebbe a questo punto responsabile del trattamento dei dati in questione.

Con la sentenza *Costeja González vs. Google*, tuttavia, la Corte di Lussemburgo ha cambiato radicalmente avviso, sostenendo che i gestori dei motori di ricerca non soltanto trattano dati ma che, ai sensi dell'articolo 2(d) D-95/46/CE, essi sono responsabili di questo stesso trattamento, nel caso di dati personali, perché "è il gestore del motore di ricerca a determinare le finalità e gli strumenti di tale attività e dunque del trattamento di dati personali che egli stesso effettua nell'ambito dell'attività medesima […] Inoltre, occorre constatare che sarebbe contrario non soltanto al chiaro tenore letterale di tale disposizione, ma anche alla sua finalità – consistente nel garantire, mediante un'ampia definizione della nozione di «responsabile», una tutela efficace e completa delle persone interessate – il fatto di escludere dalla nozione di cui sopra il gestore di un motore di ricerca per il motivo che egli non esercita alcun controllo sui dati personali pubblicati sulle pagine web di terzi" (§§ 33 e 34 della decisione).

Beninteso, questa nuova responsabilità in capo ai gestori dei motori di ricerca va ad aggiungersi a quella di coloro che hanno immesso e pubblicato dati e informazioni con pagine web, a cui, appunto, il motore di ricerca rimanda con i risultati delle ricerche svolte dagli utenti di quel servizio. La ragione che, a giudizio della corte, giustifica questo raddoppiamento di responsabilità dipende dal ruolo nevralgico che i motori di ricerca hanno finito per avere nelle odierne società ICT-dipendenti. Con le parole della Corte, "è pacifico che tale attività dei motori di ricerca svolge un ruolo decisivo nella diffusione globale dei dati suddetti, in quanto rende accessibili questi ultimi a qualsiasi utente di Internet che effettui una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti trovato la pagina web su cui questi stessi dati sono pubblicati" (§ 36 del caso).

Il risultato cui conduce il nuovo orientamento della corte, non è dunque solo che l'attività dei motori di ricerca, d'ora in avanti, va considerata sempre di per sé "attiva"; ma, proprio per questo, ricadono sui gestori di tale servizio i tradizionali obblighi sul trattamento dei dati che abbiamo introdotto in questo capitolo, sulla scorta del principio di lealtà e il modello dell'"informativa e consenso" (v. §§ 8.2 e 8.3). Oltre agli obblighi di chi carica direttamente in rete dati e informazioni personali su terzi, i motori di ricerca, in altri termini, dovrebbero "garantire che i dati personali siano «trattati lealmente e lecitamente», che vengano «rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità», che siano «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati», che siano «esatti e, se necessario, aggiornati» e, infine, che siano «conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati». In tale contesto, detto responsabile deve prendere

tutte le misure ragionevoli affinché i dati che non soddisfano le prescrizioni dettate dalla disposizione suddetta vengano cancellati o rettificati" (§ 72 della decisione).

Come se non bastasse, la Corte ammette però che in numerosi casi la tutela dei dati personali andrebbe differenziata a seconda del ruolo che le persone svolgono nella vita sociale (v. §§ 81, 97 e 99). L'interesse della pubblica opinione prevarrebbe infatti sulla pretesa individuale di vedersi tutelata la propria riservatezza, allorché si tratti di politici o persone con un rilevante ruolo pubblico. La conclusione è che i gestori dei motori di ricerca non solo dovrebbero sincerarsi se i dati offerti siano esatti, adeguati, pertinenti, aggiornati o compatibili con il diritto all'oblio degli individui, dato che "un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta [D-95/46/CE] qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati" (§ 93). In realtà, bisognerebbe aggiungere un nuovo tipo di dovere, poiché i motori di ricerca dovrebbero essere in grado di bilanciare il diritto delle persone alla tutela dei dati personali con l'esigenza collettiva di essere a conoscenza di fatti e dati rilevanti su personaggi politici o, in genere, con un ruolo pubblico.

Tra gli aspetti più importanti della decisione, sebbene la Corte non lo menzioni espressamente, va poi aggiunto quello relativo alle nuove responsabilità degli ISP, che vanno sempre integrate con le clausole d'immunità sull'e-commerce, richiamate nei paragrafi precedenti. A stretto rigore, in quanto servizio "attivo" e, per ciò, responsabile per i dati offerti agli utenti del motore di ricerca, quest'ultimo dovrebbe premunirsi che quei dati siano legittimi, proporzionati, aggiornati, ecc., ciò che evidentemente comporta che questo servizio, almeno come lo abbiamo fin qui conosciuto nel vecchio continente, smetta di esistere o diventi una versione europea del controllo preventivo invalso in altri modelli, come quello cinese (§ 8.4.3). Per scongiurare questa ipotesi, non rimane che interpretare la decisione della corte in senso "caritatevole" – al modo di Donald Davidson (1917-2003) – e cioè valorizzando quelle parti della sentenza in modo che la rendano compatibile con i principi di libertà di pensiero ed economica, sanciti dalla Carta UE e dalla normativa sul commercio elettronico.

All'atto pratico, ciò significa che i motori di ricerca non dovrebbero attivarsi preventivamente per sincerarsi se, nel caso dei 26 mila risultati processati in 0.27 secondi riguardo al mio nome, questi dati siano esatti, adeguati, pertinenti, aggiornati e compatibili con il decorso del tempo. Per non rendere il modello europeo della privacy simile alla Cina, i nuovi obblighi in capo ai motori di ricerca andrebbero piuttosto letti alla luce dell'articolo 12(b) D-95/46/CE in tema di diritto d'accesso e, più in particolar modo, del diritto dei titolari dei dati, nei confronti del responsabile del trattamento, di ottenere "a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati". Nel caso in cui questa nuova e peculiare procedura europea di *takedown notice* non venga coronata da successo, vuoi perché la richiesta dell'interessato è ritenuta infondata, vuoi perché incontra l'opposizione di terzi, vuoi perché il gestore del servizio non sa come bilanciare i diritti in gioco o si ritrovi inondato da ricorsi, rimane pur sempre aperta la strada tradizionale di adire l'autorità giudiziaria, oppure, le autorità garanti nazionali sulla protezione dei dati, in omaggio all'articolo 8.3 della Carta UE (§ 8.1.4).

Dal giorno di pubblicazione della sentenza – com'è naturale, vista l'importanza dei temi trattati – le reazioni sono state varie e divergenti. Chi ha salutato con favore l'inedito *takedown notice* europeo e, con questo, il maggior campo di tutela accordato ai cittadini in nome del "diritto all'oblio", e chi, invece, ha espresso perplessità per la lettura fornita della direttiva 46 del '95, per non dire preoccupazione per i rischi di un'ulteriore frammentazione della rete, o costernazione per alcune dichiarazioni di principio. A più riprese nelle motivazioni della decisione, in fondo, i giudici di Lussemburgo si peritano di affermare che "indubbiamente i diritti della persona interessata tutelata […] prevalgono, di norma, anche sul citato interesse degli utenti di Internet" (§§ 81 e 97-99).

Tuttavia, per cogliere adeguatamente la portata della sentenza, occorre allargare lo spettro dell'indagine e considerare l'odierno dibattito sulla riforma del modello europeo che ha preso avvio con la proposta di un nuovo regolamento della Commissione (§ 8.1.1), secondo un approccio di cui, nel bene o nel male, la Corte di Lussemburgo sembra aver tenuto conto al momento della pronuncia. Del resto, non è questa la prima volta che abbiamo visto come i giudici di una corte abbiano tenuto in considerazione il dibattito parlamentare sui temi oggetto di discussione nella lite (§ 7.2.2); e come, d'altra parte, il legislatore sia talora intervenuto per correggere le decisioni dei giudici, nel caso in cui abbiano ritenuto i loro verdetti insoddisfacenti (§§ 7.2.4 e 7.5.2). Se, per le ragioni che diremo nel prossimo capitolo, quest'ultima ipotesi non sembra applicabile al dispositivo di *Costeja González vs. Google*, rimangono nondimeno i numerosi motivi di perplessità suscitati dalla decisione sui nuovi obblighi dei motori di ricerca e sul nuovo diritto all'oblio che dovrebbe "di norma" prevalere sugli interessi degli utenti di internet. Che, poi, si registri al riguardo una convergenza tra questo orientamento della Corte e i co-legislatori di Bruxelles non fa che confermare quanto già detto dall'introduzione del libro. In sostanza, alcune tendenze in atto nel vecchio continente suggeriscono come sia il caso di fare i conti da subito con un "test di Katz" europeo.

# IX.
# *Futuri*

> "Tutti dovremmo essere interessati al futuro, dato che a tutti toccherà di passarci il resto della propria vita"
>
> Charles F. KETTERING

Ci siamo occupati nei due capitoli precedenti, dei modelli statunitense ed europeo della privacy e della protezione dei dati personali, stante la rilevanza cruciale che questi diritti hanno negli ordinamenti giuridici contemporanei. I termini del rapporto tra sicurezza nazionale e tutela dei diritti degli individui – che il contrattualismo moderno, da Hobbes (§ 2.1.2.1), a Locke (§ 3.1.1), ha posto alla base stessa delle istituzioni – sono in buona parte definiti dal diritto che gli individui, oggi, hanno in nome della loro privacy informazionale. A questa tutela va poi aggiunto ciò che un altro padre del contrattualismo moderno, e cioè Kant (§ 5.3.3.1), presentava come la libertà che spetta a ogni membro della società in quanto uomo, nei rapporti con i consimili. Al nesso tra individuo e istituzioni pubbliche, tra privacy e sicurezza nazionale, si affianca così la relazione, o il bilanciamento, tra la privacy informazionale degli individui e l'esercizio di altri diritti e libertà garantiti dall'ordinamento, come la libertà di parola o di cronaca, il diritto all'informazione, la tutela della proprietà intellettuale, ecc.

Fin qui, i due modelli di privacy, statunitense ed europeo, sono stati per lo più considerati separatamente, con il livello di astrazione introdotto con la figura 20 del capitolo sesto (§ 6.3.3). Questa indagine può essere altrimenti orientata verso il sistema complessivo delle fonti nelle società ICT-dipendenti, illustrato con la tavola 6 del capitolo quarto (§ 4.3.3.2). L'attenzione è ricaduta sulla dinamica di gubernaculum, iurisdictio, contratti e norme sociali, all'interno di un determinato sistema giuridico, come quello federale americano e quello dell'Unione europea, al fine di chiarirne le specificità. Così, per quanto concerne l'intervento del gubernaculum sul piano del diritto nazionale – cioè a dire, il primo osservabile della tavola 6 nel campo della privacy e con la tutela dei dati personali – si è vista la contrapposizione tra la vocazione settoriale del legislatore di Washington e quella, viceversa, generale del legislatore di Bruxelles, salva l'eccezione più vistosa e rilevante, a proposito della sicurezza nazionale (§§ 6.2.1 e 8.1.1).

Questo differente approccio, settoriale o generale, non può che incidere sulla sfera delle garanzie predisposte nel caso della iurisdictio: il secondo osservabile della tavola 6. Nel caso degli Stati Uniti, spetta alla Corte suprema di Washington la

tutela dei diritti costituzionali alla privacy nei confronti delle ingerenze del governo e degli stati dell'Unione, mentre la tutela del diritto nel rapporto tra privati è fondamentalmente affidata alla giurisdizione dei singoli stati: qui, possono sussistere differenze anche rilevanti tra, poniamo, lo stato del Connecticut e quello di New York, nonostante la cifra comune rimanga quella di un ambito, quello del diritto alla privacy, lasciato in larga parte all'autonomia delle parti e alle forze del mercato. Nell'Unione europea, invece, il bilanciamento tra privacy e sicurezza nazionale è per lo più affidato agli organi nazionali della iurisdictio di ciascun stato membro, laddove, per quanto attiene alla disciplina tra i privati nel settore della protezione dei dati, quegli stessi giudici sono tenuti ad applicare norme e principi del diritto UE. Nel primo caso, l'organo di chiusura giurisdizionale lo si trova, sul piano del diritto internazionale, a Strasburgo; nel secondo caso, in Lussemburgo (§ 8.1.2).

I due restanti osservabili della tavola 6, ossia contratti e norme sociali, sono stati del pari analizzati nel capitolo precedente (§ 8.3.1), per sottolineare un'ulteriore differenza tra i modelli. Sebbene negli Stati Uniti, come in Europa, i rapporti tra imprese e singoli siano regolati dai termini dei loro accordi, tuttavia, a differenza del modello americano, quello europeo impone una nutrita serie di obblighi a carico di chi raccoglie, tratta, usa o rivende dati personali ai fini più vari. In America, il più è lasciato all'auto-regolazione e disciplina delle imprese private tramite codici di condotta e termini di servizio, rispetto ai quali alcune agenzie federali hanno poteri regolativi: l'agenzia federale per il commercio, o FTC (*Federal Trade Commission*), vigila ad esempio su ciò che le imprese private promettono nelle loro stesse clausole di servizio a tutela della privacy, per cui, qualora l'impresa venisse meno ai propri impegni, ciò sarebbe "un atto o pratica sleale o fraudolenta nel, o danneggiante il, commercio" (15 U.S.C. § 45). Come detto (v. § 7), questi controlli delle agenzie federali sono però molto specifici e, per quanto la FTC abbia dichiarato di aver condotto circa trecento operazioni di controllo a tutela della privacy, "la sua giurisdizione è limitata sotto molti aspetti importanti, e non può nemmeno far valere le 'pratiche d'informazione leale' d'uso corrente negli Stati Uniti" (si v. Schwartz 2013). Per contrasto, basterebbe far caso alle decine di opinioni e raccomandazioni che il gruppo delle autorità garanti WP 29 è venuto producendo nel corso degli anni in Europa; per non parlare, poi, delle numerose sentenze della Corte di giustizia proprio in materia di tutela dei dati personali (§§ 5.4.3 e 8.4.2).

L'aver fin qui insistito sulle vistose differenze tra i due modelli propone nondimeno un'ulteriore questione, di capire cioè come questi modelli abbiano fin qui interagito; per cui conviene allargare lo sguardo dai primi osservabili della tavola 6 sul fronte del diritto interno, al diritto internazionale e transnazionale. Dai primi capitoli del libro, in fondo, si è venuto insistendo su un duplice effetto della "quarta rivoluzione"; vale a dire come i flussi dell'informazione, prodotti e favoriti dall'uso d'ICT, travalichino spesso i confini tradizionali degli ordinamenti (§ 1.4.4); e come la complessità dei temi d'affrontare – con la protezione del diritto alla privacy e la tutela dei dati personali – sia propriamente "sistemica" (§ 2.3).

Questo duplice fronte, transnazionale (§ 6.3.1) e internazionale (§ 6.3.2), della difesa dei diritti va inoltre inteso dinamicamente e, cioè, sia in rapporto ai problemi che sono rimasti aperti nell'esame dei modelli statunitense ed europeo, sia rispetto alle nuove sfide che la rivoluzione informatica promette con nuove invenzioni e ap-

plicazioni nell'ambito dell'intelligenza artificiale, della robotica, dell'"analitica dei dati" mediante il *profiling* e il *data mining*, ecc.

Sono, dunque, quattro i punti principali di cui dovremo occuparci in questo capitolo: innanzitutto (§ 9.1), è bene completare l'esame degli osservabili della tavola 6, segnalando come, fin qui, la tutela del diritto alla privacy e la protezione dei dati personali sia stata governata tra Europa e Stati Uniti, tanto sul piano internazionale, quanto transnazionale.

Dopo di che (§ 9.2), comincerà l'esame di quanto, tempo addietro (2009), WP 29 presentava come il "futuro della privacy" (doc. WP 168). Lungi dal suggerire poteri divinatori, l'esame del futuro non può che partire dai problemi d'oggi. Questi diversi problemi, cui la Commissione europea ha inteso porre rimedio con una proposta di regolamento nel 2012, possono essere riassunti con cinque punti principali, relativi al modello di governance (§ 9.2.1); ai principi del sistema, come il consenso (§ 9.2.2); ad alcune scelte legislative, come nel caso del cosiddetto diritto all'oblio (§ 9.2.3); fino ai poteri giuridici in gioco (§ 9.2.4); e i possibili usi della tecnica: è il caso della "privacy tramite design" (§ 9.2.5).

Alla luce dei problemi odierni, converrà orientarsi per prendere posizione rispetto ai "casi difficili" del diritto (§ 9.3). A tal fine, torna utile il riferimento a due tra i più noti filosofi del diritto del secolo scorso che, significativamente, tennero entrambi la cattedra di *jurisprudence* a Oxford, rispettivamente dal 1952 e, subentrandogli, dal 1969: Herbert H. Hart (1907-1992), e Ronald Dworkin (1931-2013). Riprenderemo sia la tesi di Dworkin, per cui il diritto è sempre in grado di avere un'"unica risposta corretta" anche di fronte ai casi più difficili (§ 9.3.1); sia la tesi di Hart, per cui si tratta piuttosto di mirare in questi casi a raggiungere un "ragionevole compromesso" tra i vari interessi in gioco (§ 9.3.2). In quest'ultimo caso, bisogna però affinare ulteriormente la nozione di "ragionevolezza", né più né meno come è successo con il test sulla ragionevole aspettativa di privacy svolto dalla Corte suprema negli ultimi cinquant'anni. Con l'impianto normativo offerto dall'etica dell'informazione di un altro professore di Oxford, Luciano Floridi (§ 9.3.3), sarà possibile affrontare gli altri problemi giuridici che la rivoluzione informatica è già pronta a innescare (§ 9.4). Per cominciare a cogliere come la ragionevole aspettativa di privacy sia destinata a mutare nei prossimi anni – e, di qui, come raggiungere un ragionevole compromesso tra le parti in causa – il lettore sarà orientato con tre esempi.

In primo luogo (§ 9.4.1), è il caso dei sistemi aerei di trasporto noti come RPAs (*remotely piloted aircrafts*), UAS (*unmanned aircraft systems*), oppure, più semplicemente, "droni". Questi ultimi sono destinati a mutare la nostra percezione di privacy nei luoghi pubblici, molto più radicalmente di quanto non sia fin qui occorso con altre tecnologie, come nel caso dell'impiego di CCTV (§ 5.1.2), o il GPS del caso Jones (§ 7.4).

In secondo luogo (§ 9.4.2), si farà riferimento alla robotica di servizio, con nuovi modelli di assistenti personali o di badanti artificiali intelligenti, che ridefiniranno l'aspettativa di privacy dentro le mura domestiche. Essendo queste applicazioni robotiche progressivamente connesse in rete, bisognerà aggiungere ai consueti problemi di trattamento dei dati di cui siamo già esperti, la nuova esigenza di riservatezza che sorgerà in casa propria, interagendo con una nuova classe di agenti artificiali.

Infine (§ 9.4.3), occorre ripensare radicalmente al modo in cui la tecnologia finirà per riposizionare la nostra odierna aspettativa di privacy con la convergenza di mondo reale e mondo virtuale, tra offline e online. L'esempio è offerto dal progetto della Commissione europea sui "futuri digitali" e, più in particolar modo, dall'esperienza avuta con il progetto di ricerca conclusosi nel febbraio 2013 con la presentazione dell'*Onlife Manifesto* (Pagallo 2014).

Davanti all'impatto della rivoluzione tecnologica sul diritto, la conclusione è che bisognerà mettere nuovamente alla prova il test sulla ragionevole aspettativa di privacy, per evidenziare come, finanche in un sistema giuridico diverso, rispetto a quello dove il test è nato, e cioè l'Europa, il test rimanga valido (§ 10).

## 9.1. *Blocchi di partenza*

L'ambito della protezione dei dati è uno dei settori dell'ordinamento in cui, al pari della disciplina in tema di salute, ambiente o antitrust, si è avuto il cosiddetto "effetto Bruxelles" (Bradford 2012). La tesi è che il diritto dell'Unione sia un caso unico, nell'odierno panorama delle fonti del diritto, perché, sia pure in determinati settori, il potere regolativo di un singolo attore della governance mondiale ha finito per influenzare unilateralmente gli altri stati, le organizzazioni internazionali e le forze del mercato. Tra le ragioni per spiegare questo successo, c'è da tenere in conto la dimensione economica del mercato europeo, come tale appetibile a tutte le imprese multinazionali; nonché il fatto che l'Unione europea sia dotata di una assai efficiente capacità regolativa che, nei settori di "indivisibilità degli standard" o dei parametri normativi, diventa cruciale. La normativa comunitaria in materia di tutela dei dati è infatti diventata una sorta di "asso pigliatutto" (*trump standard*), sia per l'efficacia degli strumenti regolativi, come nel caso delle opinioni e raccomandazioni delle autorità WP 29, sia per le difficoltà che le imprese avrebbero di gestire i dati personali a seconda del paese con cui intrattengono rapporti. Con le parole di Anu Bradford, questi *trump standard* "emergono soltanto quando le imprese optano volontariamente per un singolo standard globale, definito dal regolatore più severo, che rende nel frattempo le altre regolazioni obsolete" (*op. cit.*). In contrasto con altri campi che si aprono alla differenziazione del trattamento giuridico, come nel caso del mercato del lavoro, le imprese farebbero fatica a isolare, nelle proprie banche dati, le informazioni di cui hanno bisogno per svolgere un'attività mirata solo all'Europa. La conseguenza è che molte di quelle imprese hanno finito per allineare le proprie "attività globali agli standard per la privacy più impegnativi dell'Unione europea" (Bradford 2012).

L'"effetto Bruxelles" non significa, tuttavia, che la governance della privacy sia oggi rimessa alle sole decisioni delle autorità dell'Unione. Oltre agli accordi PNR ricordati nel capitolo precedente (§ 8.4.4), basta aggiungere, sul piano del diritto internazionale, gli accordi tra Stati Uniti ed Europa del 2000 su un quadro di "porto libero" (*safe harbour*) per lo svolgimento delle attività commerciali delle imprese statunitensi nel vecchio continente. Benché con l'opposizione del Parlamento, la Commissione ha infatti approvato quindici anni or sono, una serie di clausole d'immunità che vanno a integrare il marco generale esaminato poco sopra (§ 8.5.2.1), circa casi in cui le impre-

se non rispondono per le proprie attività o il comportamento degli utenti o clienti. In sostanza, il governo degli Stati Uniti e la Commissione hanno rispettivamente sottoscritto il 24 e 25 luglio 2000[1], un programma di auto-certificazione volontaria, al quale potranno partecipare le imprese e compagnie statunitensi che si impegnano di rispettare un insieme di "pratiche d'informazione leale" o FIP (*fair information practices*). Queste norme prevedono uno standard di raccolta e trattamento dei dati simile più al modello europeo, che a quello americano. In cambio di questo standard di tutela più alto, le imprese statunitensi si vedono così garantito il fatto che la maggior parte delle controversie che esse potranno avere con cittadini o enti europei, saranno discusse davanti alle corti nordamericane e sulla base dei principi giuridici di quel paese. Alle compagnie che partecipano su queste basi al programma di "porto libero" viene pertanto riconosciuto un livello "adeguato", e non solo "sufficiente", della protezione dei dati, secondo una clausola giuridica che consente che il flusso dell'informazione tra quelle compagnie americane e l'Europa sia libero come in un mercato unico.

Inoltre, le autorità WP 29 hanno messo a punto uno schema di regole vincolanti per le imprese, o *binding corporate rules* (BCR), con cui, rivedendo precedenti posizioni (doc. WP 74 del 3 giugno 2003), si snellisce il flusso transfrontaliero delle informazioni all'interno delle imprese. Nella prima raccomandazione WP 29 del 2007, sullo "standard applicativo per l'approvazione di regole vincolanti per le imprese sul trasferimento di dati personali" (doc. WP 133), era infatti predisposta la forma in cui le imprese dovevano richiedere alle autorità garanti il via libera alla circolazione di dati e informazioni, da o per l'Europa, processati da quelle imprese. Nel giugno 2008, WP 29 è tornato sul punto con un documento di domande fatte di frequente o FAQ (*frequently asked question*), al fine di risolvere, tra gli altri, problemi di competenza circa quale tra le varie autorità nazionali della privacy in Europa debba rilasciare l'autorizzazione al trattamento e trasmissione transfrontaliera dei dati alle imprese. Come informa il sito della Commissione europea, nella lista delle società per le quali la procedura di cooperazione BCR promossa dall'Unione è stata completata, troviamo multinazionali come Accenture, British Petrolium, eBay, DaimlerChrysler, Deutsche Telekom, General Electric, HP, e altri.

All'insieme della "disciplina coattiva" – o, per dirla con l'"effetto Bruxelles" di Bradford, all'"unilateralismo de facto" dell'Unione europea – nel campo della tutela dei dati, deve aggiungersi la "disciplina autoritativa" del diritto soffice come modalità regolativa d'intervento del diritto in quanto meta-tecnologia (v. figura 3 e §§ 1.1.3 e 4.3.1.1). In fondo, è ciò che ha sottolineato l'Opinione del Supervisore europeo per la protezione dati (EDPS), nel luglio 2007, a proposito del regime speciale previsto dal diritto comunitario per il trasferimento di dati e informazioni a paesi terzi, ai sensi degli articoli 25 e 26 della direttiva 46; per cui, per far funzionare al meglio tale "regime speciale", bisogna impegnarsi mediante la ricerca di clausole contrattuali standard, norme di auto-disciplina, accordi con la Camera internazionale di commercio, o con il perfezionamento del giudizio sull'adeguatezza nella tutela dei dati accordata da paesi terzi. Per dirla con Peter Hustinx, non bisogna illudersi sui poteri taumaturgici della disciplina coattiva della legge in un settore come quello

[1] Si v. il *Federal Register* e, per quanto concerne la decisione della Commissione, la 2000/520/CE.

della protezione dei dati: "questo sistema, una conseguenza logica e necessaria delle limitazioni territoriali dell'Unione europea, non garantirà la piena protezione dei dati ai soggetti europei in una società disposta a rete, in cui le frontiere fisiche perdono importanza […] L'informazione su Internet è onnipresente, ma la giurisdizione del legislatore europeo non lo è" (§ 42 dell'opinione 2007 di Hustinx).

La fitta rete di istituzioni nazionali, organi internazionali ed enti transnazionali, con la variegata serie di strumenti giuridici come direttive e leggi, raccomandazioni e opinioni, regole vincolanti per le imprese e programmi di "porto libero", non comporta evidentemente l'aver risolto né i problemi di coordinamento transfrontaliero nella tutela e controllo dei dati, né le questioni che sono venute emergendo nel frattempo, all'interno dei singoli modelli, o nei singoli sistemi giuridici nazionali. Ai dilemmi sulla tutela accordata dal sistema costituzionale americano, sotto l'egida del Quarto emendamento, già emersi con il caso Jones (§ 7.5.2), basterebbe aggiungere quelli del WP 29 nel ricordato documento sul "futuro della privacy" (doc. WP 168). In quella sede, le autorità sottolineavano i problemi incontrati dalla normativa europea sia nell'armonizzare i sistemi giuridici degli stati membri, sia nello stare al passo con l'innovazione tecnologica. All'atto pratico, WP 29 consigliava alla Commissione europea, non tanto di rivoluzionare i principi contenuti nella direttiva 46, ma d'integrarla, al fine di irrobustire i diritti dei titolari dei dati e rendere più stringenti le responsabilità di coloro che raccolgono, trattano o usano dati personali, rafforzando infine i poteri delle stesse autorità garanti (v. Pagallo e Bassi 2011).

Come detto, nel gennaio 2012, la Commissione europea è intervenuta sul punto; sebbene, sorprendendo molti, non con una direttiva, ma con la proposta di regolamento che siamo venuti menzionando nel corso dei capitoli precedenti.

Con il primo dei criteri normativi illustrati in tema di governance (§ 3.4.3.1), la Commissione ha spiegato nell'introduzione alla proposta, le ragioni e le finalità che l'hanno spinta a formulare la nutrita schiera di principi e regole contenute nel nuovo regolamento.

Con il secondo criterio sul "dovere di conoscenza" (§ 3.4.3.2), va dato atto alla Commissione di essersi presentata agguerrita alla discussione della propria proposta nel dettaglio tecnico.

Eppure, da oltre due anni si è accesa in questo modo la discussione sulla "scelta degli strumenti" (§ 3.4.3.3), sia dal punto di vista della scelta della Commissione di presentare un regolamento, piuttosto che una direttiva che sostituisse quella precedente; sia dal punto di vista del contenuto di molte delle disposizioni così presentate. Basti dire per ora che, nel processo di revisione della proposta, il Parlamento europeo ha approvato il 12 marzo 2014, più di 200 emendamenti – per l'esattezza: 207 – alla proposta di regolamento presentata dalla Commissione[2].

Si tratta di cominciare la nostra indagine sul futuro della privacy a partire dai problemi che rimangono, oggi, tuttora aperti, tra Commissione e Parlamento.

---

[2] Nel corso del capitolo, volta per volta, saranno riportati in nota gli emendamenti del Parlamento europeo che si limitano a integrare, o correggere parzialmente, la proposta normativa della Commissione. Quando, invece, detti emendamenti entrino in rotta di collisione con la proposta, gli stessi saranno propriamente discussi nel corpo del testo, tenendo anche presente, se del caso, la precedente risoluzione parlamentare del 20 novembre 2013.

## 9.2. *Problemi aperti della privacy*

Ricordava il grande economista americano John Kenneth Galbraith (1908-2006), che "l'unica funzione delle previsioni economiche è quella di far apparire rispettabile l'astrologia". Al momento di scrivere queste righe, non solo non è chiara la forma finale che avrà il testo del nuovo regolamento europeo per la protezione dei dati personali; ma, è ancora più difficile, se non impossibile, prevedere sia l'impatto che queste misure avranno nel disciplinare la materia, sia quanto o come esse potranno essere efficaci. Nondimeno, è ragionevole immaginare quali, tra le parti della proposta, saranno alla fine confermate, come ha già cominciato a fare del resto il Parlamento europeo con la ricordata delibera del 2014, secondo le linee d'intervento auspicate dallo stesso WP 29 fin dal "futuro della privacy" del 2009. In linea generale, si è trattato di intervenire nel quadro delle disposizioni vigenti in materia, sia rafforzando i diritti dei titolari dei dati, sia con nuovi obblighi per i responsabili del trattamento, come emerso nel caso dei nuovi limiti alla raccolta e uso dei dati (§ 5.3.1), o con i doveri d'informativa del responsabile del trattamento per casi di falla nei sistemi di sicurezza informatica (§ 8.2.4). Il fatto, poi, che la Commissione abbia scelto la via del regolamento, piuttosto che di una nuova direttiva in sostituzione della 46 del '95, è dipeso dalle osservazioni delle autorità garanti sui problemi di armonizzazione, posti non solo dall'avanzare della tecnologia, ma dall'allargamento dell'Unione a quasi trenta stati membri (v. documento WP 168).

In ragione di queste linee di tendenza del modello europeo sulla protezione dati, è dunque possibile ragionare attorno a quali siano i problemi aperti della privacy oggi. Ne suggerisco cinque diversi tipi che concernono in diverso modo il modello di governance, alcuni principi del sistema, il tenore di certe scelte politiche, la distribuzione dei poteri all'interno dell'ordinamento e l'uso della tecnica.

Come ben si vede, l'attenzione va innanzitutto rivolta alla "scelta degli strumenti" (§ 3.4.3.3), sul cui dibattito si è fatto cenno poco sopra, in rapporto all'alternativa tra "disciplina coattiva" e "disciplina autoritativa" del diritto come meta-tecnologia, illustrata dalla figura 3 (§ 1.1.3).

Procediamo, pertanto, con il primo problema aperto della privacy oggi, ossia quello relativo al modello di governance.

### 9.2.1. *Il modello di governance*

Ci siamo occupati di governance fin dal capitolo terzo, esaminandone sia i settori (§ 3.3.1), sia i livelli (§ 3.3.2), come risposta alla complessità crescente dei problemi con cui sono alle prese le società ICT-dipendenti. Nel capitolo sesto, questa indagine è stata ripresa e approfondita nell'ambito della privacy con la figura 19 (in § 6.2). Oltre ai problemi cognitivi e tecnologici con cui devono fare i conti le società odierne, occorre prestare attenzione agli equilibri istituzionali che si danno con la governance della privacy. Con gli osservabili della tavola 6 del capitolo quarto (§ 4.3.3.2), si è fin qui sottolineata la specifica complessità delle fonti del sistema, esaminando il fitto reticolo di attori privati e pubblici che, sul triplice piano del diritto nazionale, internazionale e transnazionale, governano la privacy contemporanea. Il riferimento va ancora una volta alle leggi, regolamenti e direttive dei legislatori nazionali; agli accordi internazionali tra

due o più stati, o con le linee guida di organizzazioni come l'OCSE; alle forme di diritto soffice, come raccomandazioni e opinioni, delle autorità garanti indipendenti; agli schemi di norme vincolanti per le imprese, predisposti da quelle stesse autorità che fungono da "impresari di politiche transgovernative" (Newman 2008); e così via.

Con la proposta di regolamento della Commissione europea, nondimeno, in molti hanno temuto, o denunciato, una "destabilizzazione dell'equilibrio" (v. Schwartz 2013). Mentre, sul piano internazionale, si avrebbe un esempio ulteriore dell'unilateralismo interventista del modello europeo – il cosiddetto "effetto Bruxelles" (Bradford 2012) – sul piano interno dell'Unione, si assisterebbe invece a una massiccia centralizzazione dei poteri regolatori da parte della Commissione, nell'avocare a sé l'ultima parola in un numero considerevole di settori d'implementazione della normativa. Lasciando per ora in sospeso quest'ultimo punto (si v. a breve § 9.2.4), molti critici del regolamento, però, ne hanno ammesso le aperture: "esso offre strade verso un nuovo bilanciamento" (Schwartz 2013). In fondo, l'intero capo V (articoli 40-45) s'incentra sul "trasferimento di dati personali verso paesi terzi o organizzazioni internazionali", dove sono fatti salvi sia gli accordi di "porto libero", sia le norme vincolanti d'impresa, illustrati poco fa (§ 9.1), aprendosi del pari alla "cooperazione internazionale" e transnazionale. Come si legge nell'articolo 45 del regolamento, l'intento della Commissione e delle autorità di controllo (WP 29, EDPS, ecc.) è di "sviluppare efficaci meccanismi di cooperazione internazionale per facilitare l'applicazione della legislazione sulla protezione dei dati personali" (art. 45 lettera (a)); "prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali" (lettera b); "coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali" (lettera c); nonché "promuovere lo scambio e la documentazione delle legislazioni e pratiche in materia di protezione dei dati personali" (lettera d) [3].

Inoltre, come diremo nel prosieguo del paragrafo, la Commissione ha saputo aprirsi all'esperienza maturata in altri ordinamenti e da altre autorità indipendenti, come nel caso del Commissario per la privacy e l'informazione in Ontario, Canada, Anne Cavoukian (n. 1952), alla quale dobbiamo, fin dagli anni novanta, la fortunata formula, poi ripresa espressamente dalla Commissione nel regolamento, sulla "privacy tramite design" (su cui ancora sotto § 9.2.5).

La conclusione da trarsi è dunque che, negli anni a venire, e al netto dell'impatto che le decisioni dell'Unione europea, tra Commissione, Parlamento e Consiglio, potranno avere sulla governance della privacy, quest'ultima, su scala globale, è destinata a rimanere fortemente policentrica e, sia pure, secondo l'ipotesi del "mondo vuoto" di Simon (§ 2.2.2.1), facente leva su alcuni grandi "hub". Riprendendo le tesi esposte nel capitolo terzo, vanno annoverati tra questi hub sia i governi nazionali sia le forme nuove d'esercizio del gubernaculum, con l'esempio dei poteri della Commissione europea. A questi hub vanno però ad aggiungersi nuovi attori istituzionali,

[3] L'unica modifica proposta dal Parlamento riguardo all'articolo 45, concerne la sua lettera (a), per cui, come si legge nell'emendamento 142, al posto di "facilitare l'applicazione", l'intento dovrebbe ora essere quello di "garantire l'applicazione della legislazione sulla protezione dei dati personali".

pubblici e privati, senza i quali non sarebbe reso un ritratto fedele della complessità che caratterizza gli odierni equilibri istituzionali. Se, esaminando nel capitolo terzo la governance d'internet, abbiamo dovuto fare riferimento a enti come l'IETF, l'ISOC, l'IAB, l'ICANN, l'IGF e altri ancora (§ 3.4.2); nel caso della privacy e con la tutela dei dati personali, il richiamo va sia alle associazioni civili sorte, tanto negli USA quanto in Europa, a tutela della privacy[4]; sia alle imprese private coinvolte nella elaborazione di codici di condotta e clausole vincolanti per le stesse imprese; sia alle forme di diritto soffice elaborate da autorità come WP 29, EDPS o, in parte, la FTC statunitense.

Questo intricato reticolo istituzionale è stato anche presentato come una "rete tridimensionale di collegamenti tra istituzioni statali disaggregate" (Slaughter 2004: 15). La crisi del modello di Westfalia ha infatti comportato che i vecchi stati nazionali non si rapportino più tra di loro come blocchi unici ma, piuttosto, tramite parti disaggregate del vecchio insieme, che provvedono ad armonizzare le regole del gioco entro il quadro definito, spesso, da accordi internazionali e, a volte, con specifici mandati legislativi al fine di ottenere uniformità ed efficienza. "Tanto più gli impegni internazionali richiedono sia l'armonizzazione o altri aggiustamenti della legge domestica, sia il coordinamento di politiche nazionali, sia la cooperazione negli sforzi d'implementazione domestica, tanto più questi obiettivi richiederanno reti di governo per far funzionare il sistema" (Slaughter 2004: 162). I meccanismi di cooperazione tra il settore pubblico rappresentato dal diritto soffice delle autorità garanti europee per la protezione dei dati, e il settore privato che negozia le clausole vincolanti d'impresa e altri meccanismi auto-regolativi per il governo della privacy, ne sono buoni esempi. Queste "reti di armonizzazione" chiamano in causa tutte le fonti delle odierne società ICT-dipendenti – v. tavola 6 di § 4.3.3.2 – sebbene con la peculiarità messa in chiaro per la governance d'internet, per cui la natura fortemente decentrata del reticolo si appoggia non di rado a pochi grandi connettori.

Tra questi hub, come detto, è apprezzabile che la Commissione abbia confermato le forme di collaborazione, internazionale e transnazionale, fin qui sperimentate, aprendo a nuovi tipi di coordinamento e, cioè, coinvolgendo tutte "le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione" (art. 45(c) della proposta).

Tuttavia, si è anche detto come molte delle disposizioni presentate dall'organo europeo abbiano suscitato perplessità o, comunque, abbiano lasciato aperti problemi e questioni, alcune delle quali particolarmente critiche. Torniamo per questo verso alla "scelta degli strumenti" cui si è fatto più sopra cenno (§ 9.2), dovendosi per ciò entrare ora nel merito dei temi che riguardano, innanzitutto, i principi stessi del sistema a tutela dei dati personali.

### 9.2.2. *L'architrave del sistema*

I principi del modello europeo sulla protezione dei dati – dal momento della loro raccolta all'anonimizzazione o definitiva cancellazione – sono stati esaminati nel

[4] Basti pensare all'ACLU e all'EFF negli Stati Uniti, alla Quadrature du Net in Francia, al centro Nexa in Italia, e via discorrendo.

capitolo precedente. Questi principi rappresentano l'architrave del sistema, rispetto alla quale devono dunque intendersi la serie di modifiche e innovazioni che siamo venuti fin qui esponendo. Come auspicato da WP 29 nel ricordato documento sul "futuro della privacy" (doc. WP 128), anche nel caso della proposta di regolamento della Commissione, l'obiettivo non è infatti di mutare radicalmente il sistema di trattamento e tutela dei dati ma, bensì, di puntellarlo; in particolare, per quanto concerne l'impianto dell'"informativa e consenso" su cui poggia larga parte del quotidiano trattamento dei dati personali (v. § 8.3.1).

La via seguíta dalla Commissione è stata fondamentalmente di rafforzare i diritti dei titolari dei dati, rendendo altresì più stringenti le responsabilità di coloro che trattano i dati, come del resto suggerito in WP 128. Sul primo fronte, l'articolo 5 del regolamento, a confronto del vecchio 6 della direttiva sui "principi relativi alla qualità dei dati", stabilisce che i dati non solo debbano essere "trattati in modo lecito, equo e trasparente nei confronti dell'interessato" (lettera a); e "raccolti per finalità determinate, esplicite e legittime" (lett. b); ma "adeguati, pertinenti e limitati al minimo necessario rispetto alle finalità perseguite" (lett. c.). Sul secondo fronte, vanno invece comprese le norme del nuovo articolo 7, a tutela del consenso degli interessati: secondo il primo punto dell'articolo, è ora il responsabile del trattamento che ha "l'onere di dimostrare che l'interessato ha espresso il consenso al trattamento dei suoi dati personali per scopi specifici". Ai sensi del quarto punto, si afferma invece che "il consenso non costituisce una base giuridica per il trattamento ove vi sia un notevole squilibrio tra la posizione dell'interessato e del responsabile del trattamento" [5].

A queste vanno ad aggiungersi altre norme nella medesima direzione: il vecchio articolo 8 sulla disciplina dei dati sensibili, divenuto articolo 9, stabilisce un regime, se possibile, ancora più stringente per il trattamento di quei dati che, ora, espressamente includono i dati genetici [6]. Inoltre, l'articolo 20 prende specificatamente di mira le tecniche già menzionate del *profiling* (§ 6.2.2): "chiunque ha il diritto di non essere sottoposto a una misura che produca effetti giuridici o significativamente incida sulla sua persona, basata unicamente su un trattamento automatizzato destinato a valutare taluni aspetti della sua personalità o ad analizzarne o prevederne in particolare il rendimento professionale, la situazione economica, l'ubicazione, lo stato di salute, le preferenze personali, l'affidabilità o il comportamento".

Il pur lodevole tentativo di puntellare il quadro originario della direttiva 46 si scontra tuttavia con i noti limiti dell'approccio imperniato sulla politica dell'"informativa e consenso" (§ 8.3.1). Per quanto la Commissione abbia inteso porre rimedio ad alcuni di questi limiti – come nel caso degli "squilibri" tra le parti in causa, se-

[5] Il Parlamento ha specificato, all'articolo 7(1), che l'inversione dell'onere della prova si attui solo nei casi in cui il trattamento dei dati avviene sulla base del consenso dell'interessato, mentre, all'art. 7(4), ha sostituito la nozione di "notevole squilibrio" con il principio che il "consenso dovrà essere limitato nello scopo e verrà meno quando detto scopo cessi di esistere o qualora il trattamento smetta di essere necessario per lo scopo per cui i dati sono stati originariamente raccolti" (emendamento 101). Per quanto concerne l'articolo 5, il Parlamento lo ha invece integrato con i principi di minimizzazione della raccolta dei dati, effettività dei diritti e integrità dei dati a mezzo di misure tecniche e organizzative (emendamento 99).

[6] Nella stessa direzione sono andate le ulteriori proposte del Parlamento: vedine l'emendamento 103. Analoghe considerazioni per l'articolo 20 riportato nel testo, di cui all'emendamento 115.

gnalato da WP 29 – rimangono gli ulteriori problemi che l'approccio dell'"informativa e consenso" pone e che sorgono dal fatto che, in realtà, è raro che gli individui possano dare il loro assenso alla raccolta e trattamento dei propri dati, sulla base di un consenso informato (Solove 2013). In fin dei conti, è già difficile immaginare che i cittadini dell'Unione europea abbiano il tempo e la voglia di leggere, con la dovuta calma, tutte le 123 pagine della proposta della Commissione con i suoi 91 articoli, cui vanno ad aggiungersi le modifiche adottate dal Parlamento europeo. Inoltre, la mole di nuove disposizioni, condizioni e presupposti per la legittimità del trattamento dei dati personali suggerisce che i termini del servizio prestato dalle imprese rimarranno, nella migliore delle ipotesi, pari alla complessità dei tecnicismi giuridici che li caratterizza al giorno d'oggi. Il risultato è che i potenziali interessati continueranno a non leggere o, leggendo, a non capire le clausole degli accordi per i quali si chiede il consenso; oppure, non saranno in grado di valutare adeguatamente i benefici e rischi che derivano dall'accordo. Esiste in fondo un'ampia letteratura scientifica che mostra come, neanche nel caso della tutela dei dati personali, i titolari dei medesimi siano i migliori arbitri dei propri interessi (Acquisti e Grossklags 2008).

Per venire incontro ai paradossi del consenso, si può ovviamente pensare alla possibilità d'inserire nuovi limiti alla validità del consenso prestato, oltre a quelli cui ha provveduto la Commissione con l'articolo 7; e cioè, invertendo l'onere della prova tra le parti, invalidando il consenso della parte più debole e via di questo passo.

Tuttavia, simile approccio renderebbe ancor più macchinoso e incomprensibile un meccanismo di tutela già alquanto imponente e, soprattutto, spingerebbe verso la china scivolosa di un insano paternalismo: il legislatore che 'dall'alto verso il basso' stabilisce la serie circostanziata di casi in cui è dato via libera agli individui di badare a se stessi sulla base del proprio consenso (§ 5.3.3).

Di qui, tra la Scilla di un consenso vacuo e la Cariddi di un paternalismo indigesto, in molti hanno cominciato a proporre di prestare più attenzione all'uso dei dati personali (§ 8.3.1). La ragione dipende dal bene giuridico che si mira a tutelare e che, anche nel settore della protezione dei dati, dovrebbe essere sempre la persona umana. Salvo trasformare la tutela dei dati nel feticcio di una protezione a sé stante, si tratta di pensare alle condizioni della raccolta, trattamento e uso dei dati personali quali forme di tutela e protezione del titolare di quei dati per i danni che possono intervenire nel ciclo vitale delle informazioni. Il baricentro del sistema di tutela si sposta in questo modo dalle olimpiche condizioni di conoscenza e informazione ottimali dell'interessato per dare l'assenso alla legittima raccolta e trattamento dei dati, all'uso concreto che s'intende fare, o si è fatto, di quei dati; nonché a quale sia l'impatto che l'uso di quei dati possa avere sul titolare. Nel tornare all'impostazione originaria del diritto alla privacy come tutela della personalità dell'individuo (§ 6.1), questo approccio, fondato sull'uso delle informazioni, non solo è suggerito dai paradossi del consenso, ma da tutti gli altri casi di riuso dei dati personali che, pur socialmente utili e legittimi, finiscono nondimeno per bloccarsi a loro volta nelle secche del consenso (§ 8.4).

L'approccio torna, sia pure in parte, anche con la proposta di regolamento che, all'articolo 33, prevede una "valutazione d'impatto sulla protezione dei dati […] quando il trattamento, per la sua natura, il suo oggetto o le sue finalità, presenta rischi specifici per i diritti e le libertà degli interessati". In particolare, si considerano

rischiosi i trattamenti finalizzati alla "valutazione sistematica e globale di aspetti della personalità dell'interessato o volta ad analizzarne o prevederne in particolare la situazione economica, l'ubicazione, lo stato di salute, le preferenze personali, l'affidabilità o il comportamento" (lettera a); oppure "il trattamento di informazioni concernenti la vita sessuale, lo stato di salute, la razza e l'origine etnica oppure destinate alla prestazione di servizi sanitari o a ricerche […] per prendere misure o decisioni su larga scala riguardanti persone specifiche" (lettera b); o "la sorveglianza di zone accessibili al pubblico […] mediante dispositivi ottico-elettronici (videosorveglianza) su larga scala" (lettera c); o "il trattamento di dati personali in archivi su larga scala riguardanti minori, dati genetici o dati biometrici" (lettera d); e, in genere, "qualunque altro trattamento che richiede la consultazione dell'autorità di controllo" (lettera e).

La lunga serie di casi in cui è prevista la valutazione preventiva sull'impatto d'uso può contribuire a una migliore tutela dei dati, ragionando sulla base del rischio che è determinato dal calcolo della probabilità degli eventi e dei danni che gli individui possono eventualmente subire, più che sulle basi di un consenso più o meno informato[7]. È inoltre possibile legittimare le misure di protezione dei dati che prescindono dal consenso degli interessati, proprio per via dell'accertata valutazione dei danni che questi ultimi subirebbero per l'uso dei dati medesimi. Come riferito (§ 8.4), questa attenzione per l'impatto d'uso, piuttosto che per l'astratta finalità per la quale i dati sono consensualmente trattati, contraddistingue l'approccio di chi affronta i temi della protezione dati dal punto di vista del raccordo di questa normativa con gli altri diritti e libertà dell'ordinamento. Le direttive sul commercio elettronico, sul diritto d'autore, sull'informazione nel settore pubblico, nei trasporti intelligenti, ecc., inducono infatti a comprendere come il riuso dei dati personali sia più o meno rischioso, o dannoso, per calibrare il modo in cui le diverse direttive in Europa vadano bilanciate.

Tuttavia, proprio la lunga e variegata serie dei casi in cui la valutazione sull'impatto d'uso è richiesta, può ingenerare un nuovo paradosso, dato che la lista può essere fuorviante, o poco intuitiva, per chi dovrebbe invece esserne tutelato. C'è infatti il rischio di smarrire per strada ciò che *justice* Harlan compendiava nella pretesa che l'individuo ha di vedersi tutelata la propria privacy (v. § 7.2.3). In fondo, molti dei casi in cui gli individui consensualmente accettano che i propri dati siano raccolti e trattati, possono recare loro danno senza, però, ricadere nella sfera di applicazione dell'articolo 33 del nuovo regolamento. L'esempio delle piattaforme sociali o gli applicativi che gli individui scaricano sui propri telefoni illustrano questo aspetto. Mentre, negli Stati Uniti, abbiamo visto come la ragionevole aspettativa della privacy, sia soggettiva sia oggettiva, funge da parametro normativo per determinare la sfera di legittimità delle attività investigative del governo, in Europa, al con-

[7] Allo stesso principio si ispirano gli emendamenti del Parlamento che, rispetto alla Commissione, propone un nuovo articolo (32 a), in tema di rischio, sulla base di nove ipotesi: tra le novità, spicca "il trattamento di dati personali concernenti più di 5000 titolari di dati protratto per ogni periodo di 12 mesi consecutivi" (emendamento 127). Al successivo articolo 33 si specifica che la valutazione del rischio "dovrà riguardare l'intera gestione del ciclo vitale dei dati personali" e "una spiegazione di quali accorgimenti di design e per default siano stati implementati ai sensi dell'articolo 23" (emendamento 129).

trario, sono i parametri fissati dal legislatore con un approccio 'dall'alto verso il basso', a precisare cosa gli individui possono pretendere che sia loro tutelato. Ma appunto, innanzi alla complessità delle disposizioni normative che definiscono questa stessa pretesa, è poi arduo stabilire come quest'ultima debba atteggiarsi.

Al senso di disorientamento degli individui, di fronte alla pletora di disposizioni e vincoli che il legislatore europeo è venuto introducendo per definire le condizioni di legittimità per il trattamento e uso dei dati personali, bisogna poi aggiungere un'ulteriore ragione che consiglia di trapiantare il test del giudice Harlan in Europa. Tornando all'ambito dell'articolo 33, lo scopo da raggiungere mediante il trapianto giuridico non è solo quello di stabilire la ragionevole aspettativa degli individui che la loro privacy sia effettivamente tutelata dal rischio nell'uso dei dati personali. Occorre in realtà mettere a confronto questa aspettativa con la ragionevolezza delle scelte legislative di Bruxelles: nel sia pur lodevole impegno di rafforzare i diritti dei titolari dei dati, rendendo più stringenti gli obblighi dei responsabili del trattamento, non mancano esempi di un intervento poco ragionevole del legislatore nella "scelta degli strumenti" (§§ 3.4.3.3 e 9.2).

In questa direzione, rinviando al prossimo capitolo forme, modalità e condizioni del trapianto giuridico, occorre cominciare a saggiare a continuazione, i profili, soggettivo e oggettivo, del test, con alcune problematiche scelte legislative, corroborate dalla iurisdictio.

### 9.2.3. *Scelte legislative*

Oltre alle scelte di carattere generale, come l'adozione di un regolamento invece di una direttiva, e mantenere l'impianto dell'"informativa e consenso" – sia pure puntellato da una nuova serie di diritti e obbligazioni in capo ai titolari dei dati e ai responsabili del trattamento – la Commissione europea è ricorsa a una serie di misure particolari, per molti versi inedite nel diritto comunitario. In aggiunta alle disposizioni cui si è già fatto cenno a proposito della qualità del trattamento, la minimizzazione dei dati raccolti, l'inversione dell'onore della prova sul consenso dell'interessato, il dovere del responsabile per il trattamento di avvertire sulle falle nelle misure di sicurezza, ecc., un'attenzione particolare meritano i nuovi diritti che la Commissione ha presentato all'articolo 17 del regolamento, ossia il "diritto all'oblio e alla cancellazione" dei dati che, in maniera oltremodo significativa, il Parlamento ha ripreso in buona parte [8].

La ragione dell'interesse è triplice:

i) si tratta per molti versi di un diritto di nuovo genere;

ii) il dibattito che questo nuovo diritto ha sollevato sin dalla presentazione della proposta di nuovo regolamento, getta ulteriore luce su un aspetto chiave del diritto

[8] L'unica eccezione rilevante è la soppressione del richiamo al "diritto all'oblio", ritenuta dal Parlamento fuorviante, per cui il nuovo insieme di diritti presentati nel testo vanno compendiati con la formula del "diritto alla cancellazione" (emendamento 112). Inoltre, si specifica la necessità che "una corte o autorità regolatrice con base nell'Unione abbia stabilito in forma assoluta e definitiva che i dati in questione debbano essere cancellati".

alla tutela dei dati; e cioè, il suo bilanciamento con altri diritti e libertà dell'ordinamento (v. § 8.4);

iii) il cosiddetto diritto all'oblio e alla cancellazione dei dati permette di approfondire l'accennata dialettica tra i profili, soggettivo e oggettivo, del test messo a punto dal giudice Harlan.

In sostanza, l'articolo 17.1 prevede che "l'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore", qualora i dati non siano più necessari per i fini per cui sono stati raccolti o trattati (lettera a); in caso di revoca o scadenza del periodo di conservazione (lettera b); opposizione dell'interessato (lettera c); o, con formula quanto meno vaga, quando "il trattamento dei dati non è conforme al presente regolamento per altri motivi" (lettera d).

Al secondo punto dell'articolo 17 sono previsti i correlativi obblighi di chi tratta quei dati, per cui "quando ha reso pubblici dati personali, il responsabile del trattamento di cui al paragrafo 1 prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione".

A questa serie di diritti (articolo 17.1) e obblighi (art. 17.2), il terzo punto prevede cinque tipi di eccezioni, nel senso che la conservazione dei dati è legittima "per l'esercizio del diritto alla libertà di espressione" (lettera a); "per motivi di interesse pubblico nel settore della sanità pubblica" (lettera b); "per finalità storiche, statistiche e di ricerca scientifica" (lettera c); nonché per adempiere obblighi legali di conservazione dei dati personali (lettera d); e nei casi in cui il responsabile possa o debba limitare il trattamento, piuttosto che provvedere alla cancellazione dei dati personali (lettera (e), che rimanda alle quattro ipotesi del successivo articolo 17.3). Per esempio, "il responsabile del trattamento limita il trattamento dei dati personali […] quando l'interessato chiede di trasmettere i dati personali a un altro sistema di trattamento automatizzato" (art. 17.3(d)). In questo caso, "il responsabile del trattamento informa l'interessato prima di eliminare la limitazione al trattamento" (art. 17.6).

Con questa nuova fitta rete di diritti, obblighi ed eccezioni, la Commissione e il Parlamento europeo hanno inteso così rispondere ai casi, sempre più frequenti, sorti nel frattempo negli stati membri dell'Unione, proprio riguardo all'esistenza o meno di un diritto alla cancellazione dei dati. A ben vedere, da un lato, tale diritto sembra potersi ragionevolmente far risalire alla tradizionale protezione dell'articolo 8 CEDU, nonché alle disposizioni della vecchia direttiva 46 del 1995; come nel caso dell'articolo 6(e) sulla qualità dei dati e, in particolare, il dovere di conservazione dei dati "per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono raccolti o sono successivamente trattati". D'altro canto, però, si è previamente notato come la rivoluzione informatica abbia profondamente inciso su questo stesso quadro per via della persistenza, replicabilità, scalabilità e rintracciabilità delle informazioni, specie su internet, insieme ai fenomeni di

de-contestualizzazione e ri-combinabilità del contenuto dei messaggi individuali (v. § 8.4). Per illustrare quest'ultimo punto, basta soffermarsi su alcune decisioni prese dai giudici nazionali sul tema, come il Tribunale di grande istanza a Parigi, la Corte di cassazione italiana, e l'Udienza nazionale di Madrid.

Nel primo caso, il 15 febbraio 2012, il Tribunale di Parigi ebbe modo di ordinare ai convenuti, Google e la sua affiliata Google.fr, di rimuovere dai servizi forniti dai propri motori di ricerca tutti i collegamenti che riportavano l'attrice della causa, la signora Diana Z., alla sua precedente vita di porno attrice. Benché quest'ultima richiesta possa apparire in contrasto con le clausole d'immunità per gli ISP chiarite in precedenza (§§ 8.4.3, 8.5 e 8.5.2.1), la corte francese accoglieva tuttavia la pretesa dell'attrice secondo una tendenza che sarebbe stata, di lì a poco, discussa anche in Italia. Il 5 aprile 2012, infatti, la terza sezione civile della Corte di cassazione affrontava nel caso 5525, le vicissitudini di un uomo politico coinvolto negli scandali italiani occorsi nei primi anni novanta del secolo scorso – noti anche come "mani pulite" – per cui, a distanza di vent'anni e dopo aver pagato il proprio debito alla giustizia, il ricorrente denunciava che tra i primi collegamenti offerti dal motore di ricerca di Google, interrogato sul proprio nome, apparivano ancora le notizie di cronaca pubblicate a quei tempi dal *Corriere della sera*. A differenza del tribunale di Parigi, la Suprema italiana non riteneva però che Google avesse il dovere di rimuovere dalle informazioni offerte dal proprio servizio, i collegamenti tra l'uomo politico italiano e le sue disavventure giudiziarie di molti anni prima. Piuttosto, in omaggio al principio che i dati trattati debbano essere "esatti e, se necessario, aggiornati" – ai sensi dell'art. 6(d) D-95/46/CE – la corte riconosceva il diritto all'oblio dell'attore e, ciò, nel senso che il *Corriere della sera* avrebbe dovuto tenere aggiornati i propri archivi: una volta che un utente di Google si voglia informare sulla vita di una persona, quest'ultima avrebbe il diritto a un quadro veritiero e aggiornato della propria storia individuale.

Il 9 marzo 2012 simili problemi sono stati analogamente discussi davanti all'Udienza nazionale di Madrid (C-131/12); ma, a differenza dei colleghi di Parigi o Roma, i giudici di Madrid sceglievano di ricorrere in via pregiudiziale alla Corte di Lussemburgo, per sciogliere tutta una serie di nodi circa l'interpretazione della normativa comunitaria per il trattamento e tutela dei dati personali, con le obbligazioni dei motori di ricerca in rete e il correlativo diritto all'oblio degli interessati. Può l'Agenzia spagnola per la protezione dati "imporre ai motori di ricerca di Google di ritirare dai propri indici il contenuto dell'informazione pubblicata da terzi, senza rivolgersi in forma preventiva, o simultanea, al proprietario della pagina web in cui tale informazione appare?" [9]. Inoltre, "i diritti di cancellazione e blocco dei dati, stabiliti dall'articolo 12(b), e il diritto di opposizione, di cui all'articolo 14(a) della Direttiva 95/46/CE, si estendono al punto di consentire al titolare dei dati di rivolgersi direttamente ai motori di ricerca per impedire l'indicizzazione delle informazioni che lo riguardano personalmente"?

Come riferito nel capitolo precedente (§ 8.5.2.2), il 13 maggio 2014 la Corte di

[9] Si tratta del punto 2.3 del rinvio pregiudiziale dell'Udienza spagnola cui segue, nel testo, l'interrogativo sollevato al punto 3.1 del documento.

giustizia ha accolto con formula positiva, tutte le richieste sollevate dal ricorrente in via pregiudiziale. Assodata la competenza della iurisdictio comunitaria a intervenire nel merito [10], la Corte di Lussemburgo ha rilevato la natura "attiva" del servizio svolto dai motori di ricerca e la responsabilità nel trattare i dati personali offerti agli utenti del servizio, innestando un'inedita procedura di *takedown notice* sulla scorta dell'articolo 12(b) della direttiva 46. Senza entrare ancora una volta nel merito dei dibattuti esiti della controversia, occorre piuttosto indugiare in questa sede sui nuovi obblighi dei motori di ricerca nel quadro predisposto dalla Commissione, in particolare con la serie di doveri per gli ISP introdotta al secondo punto dell'articolo 17 del regolamento. Qualora il testo venisse confermato, questo vorrebbe dire che, d'ora in avanti, non solo un motore di ricerca come Google, ma i servizi di Google Plus e Facebook, Twitter e mille altri ancora, dovrebbero informare gli utenti dei propri servizi del desiderio di un altro utente di far "cancellare qualsiasi link, copia o riproduzione dei suoi dati personali". È ciò tecnicamente possibile e, soprattutto, è ragionevole e desiderabile?

In primo luogo, è nota l'impossibilità di rimuovere veramente e, cioè, una volta per tutte, i dati e le informazioni immesse nella rete. Appartiene, infatti, alla natura della rete, al modo stesso in cui essa è stata pensata e funziona, la nozione di "copia" (v. Ruffo 2009). La semplice email che gli individui si scambiano ogni giorno, ad esempio, è basata sulla tecnologia di scomporre e copiare quel messaggio "a pacchetti" un numero tale di volte che quella stessa informazione, per così dire spezzettata, sarà smistata attraverso una serie di server differenti, per poi essere ricomposta nell'ultima copia che sarà letta dal destinatario del messaggio.

In secondo luogo, si può immaginare che gli ISP provvedano effettivamente a comunicare agli utenti dei propri servizi che un determinato individuo abbia manifestato, poniamo, a Facebook la volontà di essere dimenticato. Ma, nella migliore delle ipotesi, la comunicazione di Facebook farà appello solo al senso di responsabilità degli utenti di quella piattaforma sociale nell'assecondare, o meno, il desiderio della persona di esercitare il proprio diritto all'oblio.

In terzo luogo, il diritto in questione non appare nemmeno desiderabile in una serie affollata di casi, in cui occorre bilanciare quel diritto all'oblio con altri diritti e libertà tutelati dall'ordinamento, come il diritto all'informazione e il diritto a essere informati, il diritto di cronaca, ecc. È significativo, ma anche preoccupante, il fatto che il diritto di parola e la libertà d'espressione, venerati dall'ordinamento statunitense (§ 7.1), siano dalla Commissione e dal Parlamento presentati come un semplice punto in cui la conservazione dei dati è legittima (articolo 17.3(a) del regolamento). Questo approccio non soltanto è foriero di ulteriori incomprensioni tra le due sponde dell'Atlantico; ma, contrasta anche con la percezione che, più spesso, gli utenti d'internet hanno sulla ragionevole aspettativa di privacy. In fondo, il cosiddetto diritto all'oblio veicola una concezione proprietaria del passato e del ricordo delle persone, per cui spetterebbe a queste definire in qualsiasi momento quale pezzo d'informazione personale sottrarre alla disponibilità degli altri.

---

[10] Sebbene il trattamento dei dati possa avvenire, nel caso di Google, fuori dai confini dell'UE, basta, a giudizio della Corte, che lo sfruttamento economico dei dati avvenga tramite proprie filiali con stabilimento in Europa per radicare la causa nel vecchio continente: si v. § 52 della sentenza.

A volte, beninteso, questo desiderio è rispettabile, nel senso di dare l'opportunità agli individui di inserirsi in una (nuova) comunità, attraverso un nuovo inizio, una nuova storia, o la nuova vita che il diritto all'oblio assicurerebbe. È il bilanciamento tra chi ha commesso uno sbaglio, un crimine o un delitto, per il quale ha pagato il prezzo alla società – come nel caso 5525/2012 della Corte italiana di Cassazione – e l'interesse che la società può avere nel rinvangare quel passato. Anche ad accogliere il più restrittivo regime di tutela vigente in Europa, rispetto alla trasparenza che vale negli Stati Uniti anche per i precedenti penali delle persone, è però un fatto che il passato, i ricordi, o la storia, non siano certo un dato individuale, anche nel caso in cui si parli di un passato o di ricordi personali. Molti dei link, delle copie e delle riproduzioni dei dati personali che, nell'esempio di prima, Facebook chiederà ad alcuni utenti di cancellare, come risultato del desiderio di un'altra persona di non fare più parte della cerchia di amici in quella piattaforma sociale, sono infatti collegamenti, copie e riproduzioni di storie che il titolare del diritto all'oblio ha condiviso con altri.

Negli Stati Uniti, questo delicatissimo bilanciamento tra gli interessi in gioco poggia, come noto, sul primato della libertà di parola, rispetto alla quale si pongono la serie di limiti in nome della difesa nei confronti degli atti diffamatori, contro la diffusione di fatti privati o loro distorsione sotto "falsa luce". In Europa, vige come riferimento il più prudente bilanciamento dell'articolo 10 CEDU sulla libertà di espressione che, sia pure includendo "la libertà d'opinione e di ricevere o di comunicare informazioni o idee senza […] ingerenza da parte delle autorità pubbliche e senza limiti di frontiera", può essere sottoposta a "restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario" (articolo 10.2 della Convenzione del 1950).

Senza considerare, in questa occasione, le diverse giurisprudenze europee sul diritto di parola e le loro vistose differenze con il modello statunitense di protezione sotto l'egida del Primo emendamento, sembra tuttavia problematico l'intento della Commissione di far poggiare il bilanciamento tra i diversi interessi in gioco, sul nuovo diritto a essere dimenticati. La difficoltà, come detto, dipende sia da fattori tecnici, sia giuridici, sia dal contrasto del nuovo diritto con le aspettative che le persone ragionevolmente hanno sulla tutela della propria, e altrui, privacy. In aggiunta, il diritto all'oblio non fa che aggiornare le varianti del diritto come questione di "limitazione" o "controllo" sui dati e le informazioni personali (v. figura 18 nell'introduzione al capitolo sesto); che, nondimeno, sono apparse insufficienti a catturare la complessità del fenomeno. Più che di un diritto all'oblio, si tratta infatti del gravoso compito di pensare a una "giusta politica della memoria" e di ridisegnare il significato attribuito agli eventi del passato (Pagallo e Durante 2013-2014).

Del resto, a conferma delle innumerevoli questioni e perplessità sollevate dal nuovo diritto, la Commissione europea ha aggiunto un ultimo punto all'articolo 17, il nono, in cui l'organo si auto-conferisce il potere di adottare atti delegati in conformità all'articolo 86 al fine di precisare ora "i criteri e i requisiti per l'applicazione

del paragrafo 1 per specifici settori e situazioni di trattamento dei dati" (lettera a); ora "le condizioni per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico, come previsto al paragrafo 2" (lettera b); ora "i criteri e le condizioni per limitare il trattamento dei dati personali, di cui al paragrafo 4" (lettera c) [11].

Per affrontare la nuova serie di questioni sollevate dall'ultima disposizione del diritto all'oblio, bisogna passare al nuovo fronte dei problemi che la tutela dei dati personali ha aperto nel settore della privacy. Il riferimento va alla redistribuzione dei poteri giuridici in corso.

### 9.2.4. *I poteri giuridici in gioco*

Uno degli aspetti più vistosi del regolamento presentato dalla Commissione nel 2012, riguarda la serie dei poteri che l'organo europeo si è concesso in numerosi settori chiave della normativa, ben 45, secondo la stima dell'autorità garante della protezione dati di Berlino, Alexander Dix. Con le sue parole, "i poteri che la Commissione si è auto-assegnata vanno ben oltre al lecito" (in Schwartz 2013).

Come illustrato poco fa, con i poteri della Commissione nell'implementare alcune disposizioni sul diritto alla cancellazione dei dati, essa si attribuisce l'ultima parola sull'interpretazione e applicazione del regolamento in una considerevole serie di casi. Sulla base del cosiddetto "meccanismo della consistenza", ai sensi dell'articolo 62, l'organo può infatti adottare atti di esecuzione per "decidere in merito alla corretta applicazione del presente regolamento" (lettera a), "decidere sulla validità generale di progetti di clausole tipo di protezione dei dati" (lettera b), "specificare il formato e le procedure per l'applicazione del meccanismo di coerenza" (lettera c), e "specificare le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato europeo per la protezione dei dati" (lettera d).

Vero è che l'indubbia concentrazione dei poteri regolativi cui si assiste in questo modo, è stata, sia pure solo parzialmente, mitigata dagli emendamenti del Parlamento, ora limitando i casi in cui la Commissione può adottare atti esecutivi "ad applicazione generale", ora richiedendo l'opinione preventiva del nuovo "garante" sull'applicazione "coerente" del regolamento – secondo il lessico dell'articolo 66.1 – vale a dire il Comitato europeo per la protezione dei dati istituito con l'articolo 64, che sostituisce, di fatto, le funzioni fin qui svolte dal WP 29 [12].

Inoltre, nel quadro dei poteri giuridici in gioco, bisogna sempre ricordare i limiti strutturali della normativa europea in materia dei dati personali, che, come detto (§ 8.1.1), rimandano in ultima istanza alle esigenze della sicurezza nazionale e al prin-

---

[11] Il Parlamento si è limitato ad aggiungere che la Commissione abbia questi poteri "dopo aver richiesto una opinione del Comitato europeo per la protezione dati" su cui torniamo nel prossimo paragrafo.

[12] Da un lato, il Parlamento ha cancellato le ipotesi (a) e (c) di cui all'articolo 62 richiamato nel testo con l'emendamento 173. D'altro canto, all'articolo 66, il Parlamento si è auto-affiancato alla Commissione e al Consiglio nei poteri di iniziativa e consultazione con l'istituendo Comitato di cui all'articolo 64 (per una volta rimasto immodificato). Si v. infatti l'emendamento 175 approvato dal Parlamento.

cipio di sovranità degli stati membri dell'Unione. Per quanto gli equilibri possano spostarsi nei prossimi anni a favore dei poteri regolativi della Commissione, ciò non può che avvenire entro i limiti fissati dal vecchio articolo 3, e l'odierno 2, del quadro normativo.

Infine, molti dei poteri che la Commissione si è arrogata dipendono, in realtà, dal fatto che essa sembra consapevole della dinamicità e radicalità dei fenomeni in corso, a séguito della rivoluzione informatica, per cui le stesse clausole, spesso volutamente generiche, del regolamento consentirebbero una flessibilità di movimento, tramite "atti di esecuzione", sulla base del test della "consistenza", richiesta dalle sfide delle società ICT-dipendenti. La tecnica legislativa per evitare il ben noto rischio che l'intervento dell'autorità richieda di essere frequentemente rivisto per via dello stesso sviluppo della tecnologia (v. § 5.3.1), è stata così quella di adottare clausole sufficientemente vaghe e imprecise in un numero considerevole di casi, onde permettere, qualora necessario, futuri interventi da parte della Commissione.

Per chiarire quest'ultimo punto, conviene concentrarsi sul modo in cui la Commissione abbia dunque concepito il suo ruolo regolatore della tecnica e, con questo, la funzione del diritto come meta-tecnologia.

Ritroviamo in questo modo una vecchia conoscenza: il principio della "privacy tramite design" (§§ 5.4.3, 6.2.4, 8.4.1 e 8.5.1).

### 9.2.5. *I possibili usi della tecnica*

Dalla prima direttiva del 1995, l'approccio del legislatore europeo in tema di protezione dati si è ispirato al principio dell'indifferenza tecnologica della legge, nel senso che le finalità perseguite dalla normativa valgono indipendentemente dalla tecnologia impiegata (v. § 5.3.1). L'approccio è stato chiarito fin dal considerando 46 della direttiva, secondo il quale il "trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello di esecuzione del trattamento". Nell'articolo 17 sugli obblighi di sicurezza del trattamento, è però significativo che manchi proprio il riferimento alla fase della progettazione o design, concernente tali misure tecniche. A ribadire l'indifferenza tecnologica del legislatore comunitario, "gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche e organizzative al fine di garantire la protezione dei dati personali […] tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione" (art. 17.1 D-95/46/CE).

L'idea che le misure a tutela dei dati personali debbano essere presenti sin dalla fase di progettazione degli strumenti preposti al trattamento ed elaborazione dei dati, è stata ripresa e approfondita già alla fine degli anni novanta, dal garante per la privacy dell'Ontario, Anne Cavoukian. La formula compare nell'aprile 2000, nel documento sui *Privacy Design Principles for an Integrated Justice System* presentato dal Dipartimento della giustizia nordamericano e dal garante dell'Ontario (Cavoukian 2010). Qualche anno dopo, la formula è stata espressamente ripresa da WP 29 che, nella ricordata opinione sul "futuro della privacy" (2009), insiste a più riprese proprio sul "nuovo principio della privacy by design". In sostanza, l'intento è di immettere le misure a tutela dei dati personali negli strumenti preposti al trattamento ed elaborazione di quei dati, affinché, secondo il principio di minimizzazione, tali

sistemi possano raccogliere, processare e utilizzare la minore quantità possibile o, se del caso, nessun tipo di dato personale. Con gli esempi proposti da WP 29, si pensi ai sistemi di video-sorveglianza nel settore dei trasporti pubblici, che dovrebbero essere progettati in modo tale da non permettere il riconoscimento dei volti (salvo, ovviamente, per il caso di delitti); oppure, si considerino i sistemi di elaborazione dei dati negli ospedali, in cui i nomi dei pazienti ed altri elementi identificativi dovrebbero essere tenuti rigorosamente separati dai dati sullo stato di salute e relativi trattamenti medici. Con le parole delle autorità europee, "il nuovo quadro giuridico dovrà includere una norma che traduca gli odierni specifici requisiti nel più ampio e consistente principio della privacy tramite design. Questo principio dovrà essere vincolante per i progettisti e produttori di tecnologia, come per i responsabili del trattamento che dovranno decidere sull'acquisto e uso di ICT" (doc. WP 168).

Nella proposta di regolamento presentata dalla Commissione tre anni dopo (2012), le richieste di WP 29, tuttavia, sono state solo parzialmente accolte. Vero è che, allorché passa a illustrare i punti fondamentali della nuova normativa e, in particolare, gli obblighi generali dei responsabili e degli incaricati del trattamento, la Commissione spiega che "l'articolo 23 [del regolamento] enuncia gli obblighi del responsabile del trattamento derivanti dai principi di protezione fin dalla progettazione ('by design') e di default" (v. § 3.4.4.1 del documento d'illustrazione). Ma, all'atto pratico, alla luce del testo della legge, risulta chiaro che la Commissione abbia preferito attenersi al principio dell'indifferenza tecnologica del diritto. Come si legge nel considerando 66 della proposta, "nel definire le norme tecniche e le misure organizzative atte a garantire la sicurezza del trattamento, la Commissione deve promuovere la neutralità tecnologica, l'interoperabilità e l'innovazione".

Tornando all'articolo 23, il primo punto, nella versione originaria approntata dalla Commissione, riprendeva il tenore della precedente direttiva, stabilendo che "al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso, il responsabile del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, mette in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al presente regolamento e assicuri la tutela dei diritti dell'interessato". Con l'emendamento 118, il Parlamento ha specificato questa tutela con particolare riguardo "alla gestione dell'intero ciclo di vita dei dati personali" e in relazione alle finalità del trattamento e alle garanzie procedurali sull'esattezza, riservatezza, integrità, sicurezza e cancellazione dei dati, tenuto conto "dell'evoluzione della tecnica, delle migliori prassi internazionali e dei rischi rappresentati dal trattamento dei dati". Il secondo punto dell'articolo 23, a sua volta, stabilisce che "il responsabile del trattamento mette in atto meccanismi per garantire che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone", cui il Parlamento ha tenuto ad aggiungere "che gli interessati siano in grado di controllare la distribuzione dei propri dati personali".

Per quanto concerne il vecchio articolo 17 in tema di sicurezza del trattamento, esso è stato sostituito dal 30 che, non a caso, per le ragioni già viste nel capitolo pre-

cedente (§ 8.2.4), è stato uno dei più dibattuti tra Commissione e Parlamento. Pur innestando l'ormai noto meccanismo di auto-delega, la versione proposta dalla Commissione lasciava in sostanza immutato il precedente quadro normativo, nel senso che l'articolo 30.1 ripeteva la formula di rito per cui, "tenuto conto dell'evoluzione tecnica e dei costi di attuazione, il responsabile del trattamento e l'incaricato del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta e alla natura dei dati personali da proteggere". Il Parlamento, però, con l'emendamento 124, non soltanto ha proposto di tener conto della valutazione d'impatto condotta a norma del ricordato articolo 33; ma, di precisare "simile politica di sicurezza" tramite "la capacità di assicurare che sia convalidata l'integrità dei dati personali", nonché "la capacità di ripristinare la disponibilità e l'accesso ai dati in modo tempestivo", oltre alla capacità di adottare azioni di prevenzione, correzione e attenuazione, praticamente in tempo reale" nel caso dei dati sensibili, ecc.

Inoltre, sempre con l'emendamento 124, il Parlamento ha pensato bene di negare alla Commissione il potere che essa aveva provato a conferirsi ai sensi dell'articolo 30.3, vale a dire "di adottare atti delegati […] al fine di precisare i criteri e le condizioni concernenti le misure tecniche e organizzative di cui ai paragrafi 1 e 2, compresa la determinazione di ciò che costituisce evoluzione tecnica, per settori specifici e in specifiche situazioni di trattamento dei dati, in particolare tenuto conto degli sviluppi tecnologici e delle soluzioni per la protezione fin dalla progettazione e per la protezione di default". Questo potere di stabilire "ciò che costituisce evoluzione tecnica" e le "soluzioni" che la tecnologia può offrire per la protezione dei dati tramite design e di default, viene ora affidato al potere soffice del Comitato europeo per la protezione dei dati attraverso "linee guida, raccomandazioni e pratiche di riferimento [*best practices*] ai sensi dell'Articolo 66.1(b)" del regolamento.

Nondimeno, sia che si tratti del testo messo a punto dalla Commissione, sia che si abbia invece a che fare con gli emendamenti del Parlamento, ciò che è rimasto aperto è il problema di stabilire quali possano essere i fini di questa politica europea della privacy tramite design e di default [13]. Come chiarito nel capitolo quinto (§ 5.2), occorre far leva sul disegno della tecnologia per invogliare gli individui a mutare il loro comportamento? Oppure, secondo l'approccio tradizionale degli articoli 17 (vecchia direttiva) e 30.1 (nuovo regolamento), l'obiettivo rimane quello di ridurre l'impatto dei potenziali eventi dannosi dell'interazione umana con la progettazione di adeguate misure di sicurezza? E, però, che ne è dell'intento di prevenire del tutto la possibilità che un presunto evento dannoso si verifichi a causa del design?

---

[13] Secondo l'emendamento 118 del Parlamento all'articolo 23 della proposta, ricordato sopra nel testo, "la protezione dei dati fin dalla progettazione [*privacy by design*] presta particolare attenzione alla gestione dell'intero ciclo di vita dei dati personali dalla raccolta al trattamento alla cancellazione, incentrandosi sistematicamente sulle garanzie procedurali generali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza fisica e alla cancellazione dei dati personali". Nonostante l'ampiezza della formula e il suo appello a "garanzie procedurali generali", rimangono però intatte le difficoltà tecniche di programmare sistemi informatici che tengano conto del contesto dei rapporti. Inoltre, bisognerebbe aggiungere i vicoli ciechi del paradigma del consenso e, tutto sommato, la finalità ultima che il design finisce per assumere in questo modo, tra fini di sicurezza e autonomia delle scelte.

Per chiarire ulteriormente i dilemmi delle istituzioni europee, valga l'esempio di chi, in fondo, ha inventato la formula della "privacy tramite design", al fine di affrontare le sfide dei "sempre crescenti effetti sistemici" delle ICT e dei sistemi informativi su larga scala e a rete (Cavoukian 2010). Dopo oltre dieci anni di sforzi e crescente successo, organizzando l'"incontro definitivo" sul principio nel novembre 2009, il garante dell'Ontario ne riassumeva il concetto in ragione di sette punti chiave:

i) la protezione dei dati personali deve avvenire in forma proattiva, più che reattiva, nel senso che l'approccio della privacy tramite design ha uno scopo preventivo e non, semplicemente, correttivo o curativo;

ii) i dati personali devono essere automaticamente protetti in ogni sistema informativo (ICT), come configurazione base, o di default, del sistema;

iii) la protezione dei dati deve per ciò essere implementata nella progettazione o design dei sistemi informativi;

iv) la piena funzionalità del principio che discende da (ii) e (iii), mira a conseguire una tutela che sia vantaggiosa per tutti e che, comunque, renda superfluo, o inutile, qualsiasi altro abituale tipo di compromesso o bilanciamento tra gli interessi in gioco: ad esempio, il classico scambio tra privacy e fini della sicurezza;

v) la protezione dei dati deve coprire l'intero ciclo vitale dell'informazione, ossia dalla culla alla tomba, come nella figura 25 di § 8.4; per cui le misure a tutela dei dati devono essere predisposte ancor prima che un singolo dato, o pezzo d'informazione, sia stato raccolto;

vi) a prescindere dal tipo di tecnologia o pratica imprenditoriale, il disegno e la programmazione dei sistemi deve rendere i meccanismi di protezione dei dati visibili e trasparenti sia per gli utenti d'ICT sia per i loro fornitori;

vii) il principio richiede infine che "architetti e operatori abbiano innanzitutto a cuore gli interessi dell'individuo, nell'offrire misure quali rigorose impostazioni predefinite [default] del sistema, informativa appropriata e opzioni che siano amichevoli per l'utente e lo rafforzino" (Cavoukian 2010). In altre parole, la privacy tramite design richiede d'incentrarsi sul rispetto per l'individuo e a tutela della privacy dell'utente.

Concentrando l'attenzione soprattutto sui punti (ii), (iii) e (v) dello schema di Cavoukian, tuttavia, tornano le preoccupazioni espresse sul fine del design a "controllo totale" (v. §§ 5.2.3, 5.3.3 e 5.4). Rispetto alle considerazioni generali svolte in quella sede, il caso particolare di un'automatica privacy tramite design conferma le ragioni per cui, sia dal punto di vista tecnico, sia etico, sia giuridico, l'applicazione automatica della legge appare a dir poco problematica. In chiave tecnica, il settore della protezione dati presenta concetti come "dato personale", "responsabile" o "misura di sicurezza", che spesso dipendono dal contesto in cui vengono situati e che, comunque, allo stato attuale della ricerca e sviluppo tecnologico, risultano difficilmente programmabili in modo tale, che anche un sistema informativo o una macchina possano processare correttamente questa informazione. In chiave etica, bisogna poi rammentare il ruolo che le scelte personali svolgono nel caso della privacy, per cui gli individui modulano diversi livelli di accesso e controllo sulle informazioni personali, a seconda del contesto e delle circostanze, che risultano tuttavia difficili da conciliare con il punto (v) dello schema di Cavoukian. In chiave giuridi-

ca, infine, l'applicazione automatica del diritto alla tutela dei dati personali solleva ulteriori contrasti con i principi dell'*habeas data* europeo – come nel caso del principio all'"auto-determinazione informativa" degli individui sancito dal Tribunale costituzionale tedesco – perché in conflitto con la sfera di autonomia che deve essere riconosciuta al titolare dei dati.

La versione automatica del principio della privacy tramite design non fa per ciò che rinforzare i dubbi sulla desiderabilità (§ 5.4.1), fattibilità (§ 5.4.2), e legalità (§ 5.4.3), dell'approccio. Sebbene esistano numerosi esempi e campi in cui l'obiettivo d'immettere i comandi della legge nei prodotti e processi dell'interazione umana torni effettivamente utile, come nel caso dei sistemi CCTV, nella prevenzione della perdita dei dati o nella configurazione dei sistemi d'interfaccia per le piattaforme sociali (Pagallo 2012, 2012a), si comprende tuttavia la prudenza fin qui dimostrata dalle istituzioni europee rispetto a un principio che ben può tradursi in una forma nuova, e tecnologicamente raffinata, di paternalismo (§ 5.3.3.2). La Commissione, nel citare espressamente il principio, sia al punto 3.4.4.1 del documento con cui illustra e presenta il nuovo regolamento, sia agli articoli 23 e 30 del medesimo, ha presentato una versione sufficientemente ampia, o vaga, del principio, tale da poter comprendere i tre fini che il design può avere: sospingere gli individui a modificare il proprio comportamento, attenuare l'impatto di eventi dannosi, o prevenire del tutto la possibilità che questi eventi dannosi si verifichino. Nonostante il Parlamento sia poi intervenuto con i propri emendamenti, ora cancellando parte dei poteri esecutivi che la Commissione si era attribuita, ora affidando parte di queste competenze al potere soffice del Comitato per la protezione dei dati, i numerosi riferimenti che il Parlamento fa al principio della privacy tramite design e alla neutralità tecnologica della legge, non ne precisano univocamente la portata o il significato. Nel lasciare uno spazio di manovra piuttosto ampio per adottare "atti esecutivi ad applicazione generale" nel corso dei prossimi anni, bisognerà dunque vedere quale anima delle istituzioni europee potrà prevalere. Nel caso della Commissione, prevarrà quella draconiana dei sistemi di filtraggio onnipervasivo (§ 5.2.3); o quella garantista per l'attività di polizia e la giustizia penale (§ 5.4.3)? Nel caso del Parlamento, dopo le elezioni del maggio 2014, prevarrà l'anima liberale o, dopo la bocciatura della Corte di giustizia, torneranno alla carica i falchi della ritenzione dei dati (§ 8.4.4.1)?

A ben vedere, dopo il plesso di questioni sul modello di governance, sui principi consensuali del sistema, con alcune difficili scelte sul diritto all'oblio e con la tentazione di accentrare i poteri regolativi all'interno del diritto europeo, sembra chiaro perché il principio della privacy tramite design sia destinato ad accendere il dibattito anche nei prossimi anni. Si tratta del quinto ordine dei problemi aperti nell'odierno panorama della tutela dei dati personali, che s'intrecciano con le forme nuove in cui il diritto alla privacy va evolvendo negli ordinamenti giuridici contemporanei.

## 9.3. *Casi difficili*

Ci sono fondamentalmente due modi opposti, secondo cui possiamo affrontare la serie di problemi aperti nelle precedenti pagine. Il primo è quello proposto da

Ronald Dworkin, per cui, per ciascuna delle questioni rimaste irrisolte, sarebbe sempre possibile pervenire a un'"unica risposta corretta". Per Herbert Hart, al contrario, si tratterebbe di trovare un "ragionevole compromesso" per alcune, almeno, di quelle stesse questioni. A rendere ancora più intricati i termini del problema, si tenga poi presente l'impatto della rivoluzione tecnologica, sia sui profili cognitivi e sugli istituti del diritto, sia sulle tecniche e le sue istituzioni (figura 4 di § 1.4): spesso, come ricorda appunto il caso della privacy, siamo innanzi a questioni inedite, dovute al riposizionamento tecnologico dell'istituto (§ 6.1).

Il compito del presente paragrafo è pertanto quello di orientarci rispetto ai mutamenti e problemi in corso, alle luce dei nuovi osservabili dell'analisi illustrati dalla figura 28.

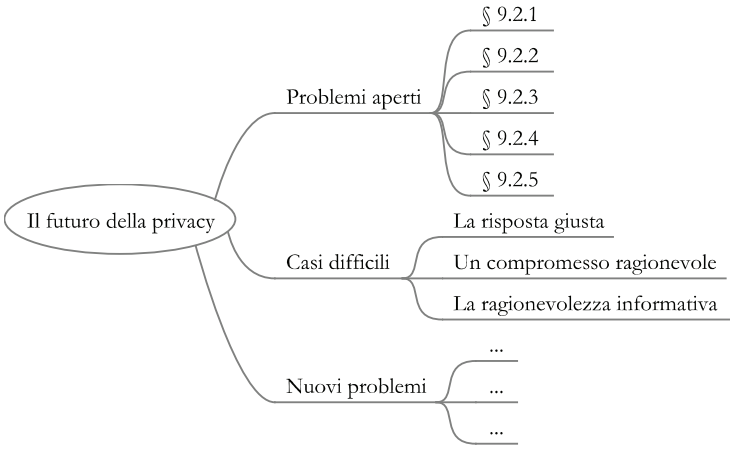


Figura 28: *I casi difficili della privacy*

Senza avere la pretesa di esaurire i problemi segnalati in precedenza ma, piuttosto, affinché il lettore trovi il modo di affrontarli in rapporto a una coerente cifra teorica, occorre approfondire a continuazione i tre nuovi osservabili della figura. Essi riguardano, rispettivamente, la tesi della "risposta corretta" di Dworkin (§ 9.3.1), quella del "ragionevole compromesso" di Hart (§ 9.3.2), e l'etica dell'informazione del terzo filosofo oxoniense di questo paragrafo, ossia Luciano Floridi (§ 9.3.3).

Su questi basi, potremo visionare i nuovi problemi della privacy che ci attendono nel futuro (§ 9.4).

### 9.3.1. *La risposta giusta*

Della ricca e variegata opera di Dworkin, limitiamoci a considerare i fondamenti teorici della tesi per cui, innanzi a un problema giuridico dato, sarebbe sempre possibile pervenire a un'unica risposta "giusta", nel duplice senso di ciò che è privo di errori o di difetti, perché è corretto (*right*); e di ciò che è oggettivamente valido per tutti, perché è buono. Davanti al numero di questioni aperte, esaminate nei paragra-

fi precedenti, occorrerebbe così interpretare il diritto, al modo di Dworkin, in forma moralmente coerente affinché, definita la natura del problema giuridico e il suo contesto, o sfondo storico, lo studioso possa trovare la soluzione che meglio giustifichi, o si accordi con, l'"integrità" della legge. Secondo il parallelo che il filosofo americano scorge tra diritto e letteratura, bisogna infatti pensare agli esperti di diritto come un "gruppo di scrittori" che, uno dopo l'altro, si susseguono per comporre un racconto collettivamente. Ciascuno scrittore della catena interpreta i capitoli del racconto già scritti, per stendere a sua volta il capitolo successivo che sarà poi aggiunto a ciò che il prossimo scrittore avrà in sorte, e così via: dobbiamo "leggere attraverso ciò che gli altri giudici hanno scritto nel passato, non soltanto per scoprire ciò che quei giudici hanno detto, o il loro stato mentale quando lo hanno detto, ma per raggiungere un'opinione su ciò che quei giudici hanno fatto collettivamente, nello stesso modo in cui ciascuno dei nostri scrittori si è fatto un'idea sul racconto collettivo che, fin qui, è stato composto" (Dworkin 1985: 159).

Anche senza accogliere i presupposti teorici e ideologici della tesi di Dworkin – che, pensando soprattutto alla tradizione di common law, declina la natura del diritto in chiave ermeneutica, come interpretazione letteraria – si può tuttavia concedere che il suo metodo colga la forma in cui i giuristi affrontano effettivamente la maggior parte dei problemi con i quali sono alle prese ogni giorno. Un esempio del metodo, in fondo, lo si è avuto nel capitolo quinto, esaminando i problemi di legalità sollevati dall'uso del design a controllo totale (§ 5.4.3); oppure, nel capitolo ottavo, prendendo posizione sul regime d'immunità previsto per i fornitori di servizi in rete (§ 8.5.2). Davanti a una specifica questione giuridica, bisogna muovere dai principi in gioco e dal retroterra storico dei problemi che occorre risolvere, per offrire la risposta che sappia garantire la finalità della legge al suo massimo grado. Si tratta di ciò che, nell'*Impero del diritto*, Dworkin idealizza con la figura di Ercole, giudice dotato di tempo e conoscenze illimitati, e per ciò capace di comprendere appieno le finalità dell'ordinamento e le molteplici implicazioni dei principi in gioco con le varie interconnessioni tra le leggi. Da questo punto di vista olimpico, c'è dunque sempre un unico modo di applicare la legge nella forma migliore possibile, e questo è il modo necessariamente prescelto dal giudice Ercole per garantire l'equità, integrità e giustizia del sistema. A ben vedere, chi tra i giuristi non ambirebbe alla sapienza di Ercole?

Nel corso delle pagine e capitoli precedenti, tuttavia, abbiamo visto una classe ulteriore di casi che sembra resistere all'onniscienza di Ercole. Per rimanere nell'ambito della protezione dei dati personali e del diritto alla privacy, si pensi solo all'architrave del sistema, ossia all'impianto dell'"informativa e consenso" (§ 9.2.2). Per quanto possa esserci l'accordo sulla necessità di integrare questo approccio, badando all'uso che dei dati personali si può fare in termini di rischio, rimangono nondimeno molte opzioni aperte sul modo in cui l'architrave del sistema di tutela può conseguentemente essere ri-bilanciato (§ 9.2.3). Allo stesso modo, le diverse forme in cui la tutela della privacy informazionale è di fatto bilanciata con il diritto di parola negli Stati Uniti e negli stati membri dell'Unione europea, difficilmente sembrano riconducibili a un unico modello, o risposta giusta, con cui definire chi, tra americani ed europei, abbia ragione. Dopo tutto, a questo medesimo tipo di difficoltà sembra far capo lo stesso Dworkin, quando ammette che "per ogni via intrapresa da Ercole, muovendo dalla sua concezione generale al verdetto particolare, un

altro avvocato o giudice che parta dalla stessa concezione, potrebbe trovare un cammino diverso e finire in un luogo differente, come molti dei nostri giudici negli esempi illustrati in precedenza hanno fatto. Quel giudice o avvocato concluderebbe in modo diverso, avendo preso commiato da Ercole, nel seguire le proprie intuizioni, prima o poi, a un certo bivio dell'argomentazione" (Dworkin 1986: 412).

Possiamo dunque seguire la via indicata da Dworkin, tenendo ferma la promessa di non aggiungere un'ulteriore versione di ciò che il diritto è, o come debba essere (§ 1.1.2). Abbiamo fin qui esaminato come il diritto si riposizioni nell'era della "quarta rivoluzione", cercando volta per volta la soluzione che meglio giustifichi, o si accordi con, l'"integrità" della legge. A differenza di Dworkin, però, l'intento di presentare il diritto sotto la sua miglior veste, in maniera moralmente coerente, non comporta che esso sia veramente una forma d'interpretazione letteraria, o che i principi del sistema consentano sempre di trovare l'unica risposta corretta al problema affrontato. Anche a seguire le indicazioni di Dworkin, si finisce infatti per incontrare, prima o poi, alcuni bivi o diramazioni nell'argomentazione giuridica, per cui sono richieste risposte politiche, più che di stretto diritto, alle difficoltà in cui va a parare di tanto in tanto l'ordinamento. Nel capitolo settimo, si è del resto osservato come tanto i giudici (*justice* Alito), quanto la dottrina (Orin Kerr), ritengano che si dovrebbe lasciare al potere legislativo il compito di fornire le norme primarie con cui disciplinare l'interazione sociale quando la tecnologia è in flusso (§§ 7.4.1.1 e 7.5.2). Davanti a una rivoluzione tecnologica, come quella odierna, sarebbe per ciò preferibile puntare su quanto il predecessore di Dworkin alla cattedra di filosofia del diritto a Oxford, Herbert Hart, presentava come un "ragionevole compromesso". Sul piano del diritto come metatecnologia (§ 1.1.3), vediamo in cosa consista l'alternativa alla tesi dell'unica risposta corretta.

### 9.3.2. *Un compromesso ragionevole*

In uno dei testi di filosofia del diritto più influenti degli ultimi cinquant'anni, *Il concetto di diritto* (1961), Hart offre l'alternativa alla teorica dell'unica risposta corretta, sulla base della distinzione tra casi semplici e casi difficili. La tesi di Hart è che il più delle volte, per nostra fortuna, i concetti del diritto abbiano un "nucleo certo" di significato, stante il quale, nonostante l'intricata rete di nozioni, principi e forme argomentative, i giuristi vengono a capo di tutta una serie di casi, in cui i termini generali non sembrano aver bisogno d'interpretazione, tanto sono "automatici" (Hart ed. 1994: 123). Tra i tanti, basti citare l'esempio della responsabilità giuridica illustrato con la figura 27 in § 8.5, per cui non è affatto problematico che in certe circostanze il concetto s'intrecci con la responsabilità morale degli individui e in altri invece la ignori, secondo una configurazione a priori o a posteriori dell'istituto che al giurista, appunto, finisce per apparire del tutto naturale.

Ciò non toglie che, a giudizio di Hart, il diritto presenti una struttura aperta, nel senso che siano lasciate a una successiva risoluzione ad opera del legislatore, o dei giudici, i modi di affrontare "questioni che possono essere bene valutate e sistemate soltanto" in un momento successivo o "quando sorgono in un caso concreto" (Hart ed. 1991: 153). Si tratta di trovare un equilibrio tra la certezza delle disposizioni di legge e la necessaria flessibilità dell'ordinamento, cui il legislatore può mirare attra-

verso una pluralità di tecniche, come l'uso di clausole generali nel testo della legge – come nel caso del principio di lealtà del trattamento (§ 8.1.4) – o riservandosi di integrare il testo tramite successivi atti esecutivi, come nel caso della Commissione (§ 9.2.5). Nella prima ipotesi, possiamo immaginare che, nonostante l'uso di clausole generali, "vi saranno degli esempi chiaramente indiscutibili che li soddisfanno o non li soddisfanno" (Hart 1991: 154). Ad esempio, nel caso del principio di lealtà del trattamento, è dato concepire sia l'individuo responsabile del trattamento che ottemperi a tutti i doveri d'informativa e sicurezza previsti dalla legge, sia colui che viceversa rivende illecitamente dati personali, o li usa per finalità differenti da quelle concordate, ecc. Ma, prosegue Hart, "questi sono solo i casi estremi di una serie di fattori diversi […] in mezzo ad essi stanno i difficili casi reali che richiedono attenzione" (*ibidem*). Quanto alla seconda ipotesi, e cioè quando c'è "bisogno di una ulteriore scelta di carattere ufficiale […] è chiaro che l'autorità normativa deve esercitare una certa discrezionalità, e non è possibile trattare la questione sollevata dai diversi casi come se fosse possibile trovare una sola soluzione corretta, che non sia un ragionevole compromesso tra molti interessi in conflitto" (*op. cit.*, 155).

In termini generali, seguendo gli assunti de *Il concetto di diritto*, ci sono tre casi in cui il disaccordo tra i giuristi non solo sfocia in un caso difficile, ma può essere risolto soltanto con un compromesso ragionevole. Il disaccordo può infatti vertere innanzitutto sugli stessi principi del sistema giuridico, sia rispetto al loro bilanciamento, come nel caso emblematico della privacy rispetto alle esigenze della sicurezza pubblica (§§ 6.2 e 8.1), sia rispetto alla logica secondo cui i principi stessi vanno intesi. Alla logica di chi, come Dworkin, si appella ai principi per offrire la risposta che sappia garantire la finalità della legge al massimo grado, si oppone chi attribuisce ai principi un significato deontologico, per cui, in quanto proposizioni normative, i principi ubbidirebbero alla logica del si o del no, ossia del "buono per tutti", piuttosto che alla logica del bilanciamento, tra il più e il meno, o "buono per noi" (Habermas 1995).

In secondo luogo, il disaccordo che sfocia in un caso difficile può riguardare i concetti giuridici in gioco, come nell'esempio di "dato personale" (§ 5.3.1). La vecchia definizione dell'articolo 2, lettera b, della D-95/46/CE, aveva infatti dato il via a una serie interminabile di dibattiti su cosa mai dovesse intendersi come "personale" rispetto al dato in innumerevoli casi. Con la nuova formula di "insiemi di dati personali", come visto, la Commissione ha inteso porre riparo alla disparità di vedute, sostituendo l'articolo 2(b) con il 4(3) della proposta di regolamento in tema di definizioni.

In terzo luogo, la difficoltà può dipendere dalle forme dell'argomentazione giuridica e, cioè, dal diverso modo in cui i molteplici concetti giuridici sono tra di loro connessi, per decidere il caso. Tornando all'esempio della responsabilità giuridica, ci sono campi, come quello della responsabilità penale, in cui, in omaggio al principio di legalità, non è lecito ricorrere a forme di interpretazione analogica; invece, altri casi suggeriscono che sono le analogie a orientare il ragionamento dei giuristi nell'affrontare problemi attinenti ora alla responsabilità civile (§ 8.5.2), ora alla tutela dei diritti umani (§ 4.3.2.1). Tuttavia, può essere finanche impossibile distinguere quando, tra le due classi di casi per cui l'impiego dell'analogia è consentito, o meno, si ricorra a un'interpretazione estensiva, più che analogica, della legge (v. Bobbio 1938).

Rispetto a questi tre ordini di casi difficili, dunque, la tesi di Hart è che i vicoli ciechi e i problemi in cui, talora, vanno a parare gli ordinamenti giuridici, richieda-

no una soluzione politica, più che di stretto diritto, che giunga a un ragionevole compromesso tra le diverse opzioni e interessi in gioco.

A rendere il caso, se possibile, ancor più difficile, c'è però da aggiungere che la nozione di ciò che è "ragionevole" appare destinata a diventare essa stessa problematica, per via dell'impatto della tecnologia con la "quarta rivoluzione". Con l'esempio della nozione di responsabilità giuridica, basta far caso al terzo osservabile della figura 27 in § 8.5. Tradizionalmente, le forme penali e civili di responsabilità giuridica che dipendono dalle circostanze del caso, fanno capo alla figura della "persona ragionevole" e, cioè, capace di prevenire il danno che sia "prevedibile". Si tratta di un approccio che risale alle radici della nostra tradizione filosofica, con la definizione aristotelica delle scienze pratiche che, come nel caso del diritto, hanno a che fare con ciò che accade per lo più nelle faccende umane (§ 1.1.1). Questo consolidato approccio alla ragionevolezza rischia tuttavia di cogliere la maggior parte degli individui impreparata a condividere un nuovo ambiente globale fatto d'informazione – l'infosfera – sia con gli organismi biologici, sia soprattutto con gli agenti artificiali (§ 1.4). Nel caso della privacy e della protezione dei dati personali, si tratta del riposizionamento in corso, dopo le banche dati, i satelliti, o i sensori termici, con una nuova generazione di enti artificiali intelligenti. Valga, per tutte, la copertina che l'autorevole settimanale inglese *The Economist* ha voluto dedicare il 28 marzo 2014 a "The Rise of the Robots".

Il ragionevole compromesso di Hart chiama perciò in causa le decisioni politiche che ci attendono sul fronte della riforma del modello di tutela della privacy, fondato sull'"informativa e consenso", man mano che i due mondi del reale e del virtuale convergano. Nel capitolo quinto (§ 5.3.1), si è avuto occasione d'introdurre questo aspetto del problema, sottolineando i diversi modi in cui è dato intendere la neutralità tecnologica delle scelte giuridiche. A continuazione, bisognerà invece cogliere come la convergenza tra offline e online possa incidere sulla ragionevolezza dei compromessi che saranno resi necessari dai nuovi casi difficili prodotti dalla tecnologia. Dopo il richiamo a Dworkin e Hart, occorre proseguire l'analisi, rifacendoci al terzo filosofo oxoniense di questo paragrafo, vale a dire Luciano Floridi.

### 9.3.3. *La ragionevolezza informativa*

Possiamo cominciare a chiarire ciò che appare "ragionevole" nell'era della quarta rivoluzione, tornando alle tesi e assunti dell'etica dell'informazione di Floridi, introdotti già nel capitolo primo (v. § 1.4).

Si tratta in sostanza di un approccio che, ai fini della presente analisi, può essere convenientemente illustrato sulla base di tre punti principali (v. Pagallo e Durante 2009): il richiamo va all'onto-centrismo della teoria, rivolta al paziente, in chiave ecologica o unitaria. Specificamente:

i) abbiamo innanzitutto a che fare con una prospettiva onto-centrica e, cioè, basata sull'essere, più che su un rigido antropocentrismo metodologico: ciò significa che occorre adottare un'ottica più ampia di quella tradizionalmente imperniata sul ruolo degli agenti umani;

ii) segue di qui una diversa comprensione dell'interazione tra agenti e pazienti, o destinatari delle azioni, in ragione del livello di astrazione che assume tutte le entità

in termini d'informazione: "tutte le entità, in quanto oggetti informazionali, hanno un intrinseco valore morale, benché anche minimo e sormontabile, per cui essi possono contare come pazienti morali, soggetti a qualche grado, parimenti minimo, di rispetto morale, inteso come una forma di attenzione disinteressata, attenta e grata" (Floridi 2008: 21);

iii) l'intento della teoria non è soltanto di spiegare come gli agenti comunichino e condividano risorse informative tramite messaggi positivi o negativi: per il taglio onto-centrico della teoria, l'etica dell'informazione mira a fornire una prospettiva unitaria per i vari stati e regimi che concernono il contenuto di tali risorse, indipendentemente cioè da specifiche tecnologie e in una forma imparziale e universale.

Ciò che Floridi definisce come il "principio di eguaglianza ontologica" vuol dire che le risorse del sistema sono intese come enti informazionali che devono essere trattati moralmente come parti dell'ambiente, o infosfera, portando a "definitivo compimento il processo di estensione del concetto di ciò che può valere come centro di rivendicazione morale" (Floridi 2008: 12). Un quadro normativo universale dovrebbe pertanto governare l'intero ciclo vitale dell'informazione sia indipendentemente da un particolare settore di indagine, come nel caso della tutela dei dati personali (figura 25 di § 8.4); sia in ragione del principio di eguaglianza ontologica, in forma imparziale.

Più in particolare, il quadro normativo fa leva sul concetto di "entropia informativa". Il riferimento va a "ogni tipo di distruzione o corruzione di oggetti informazionali (si badi, non d'informazione), ossia, ogni forma d'impoverimento dell'essere" (Floridi 2008: 11), secondo un principio sviluppato in ragione di quattro leggi morali. Esse sono:

a) non bisogna creare entropia nell'infosfera;
b) occorre prevenire l'entropia nell'infosfera;
c) si deve rimuovere l'entropia dall'infosfera;
d) bisogna promuovere la prosperità degli enti informazionali, così come di tutta l'infosfera, preservando, coltivando, aumentando o arricchendo le loro proprietà.

Alla luce di queste leggi morali, è dato precisare la nozione di ragionevolezza, sottesa ai compromessi resi necessari dai casi difficili del diritto, al modo di Hart. In termini ancor più generali, possiamo aggiornare il discorso fin qui svolto sulla scia del costituzionalismo moderno con l'idea di contratto sociale, tanto nella variante sinallagmatica offerta dal giusnaturalismo di Locke (§ 3.1.1), quanto nell'accezione democratica della volontà generale di Rousseau (§ 3.1.2). Con Dworkin, si può infatti assumere l'etica dell'informazione come la premessa moralmente coerente dell'analisi con la quale, definita la natura del problema giuridico e il suo contesto storico, si mira a individuare la soluzione che meglio giustifica, o si accorda con, l'"integrità" della legge. Così, nel caso del contrattualismo di Locke, lo scambio tra la rinuncia al diritto naturale di farsi giustizia da sé e la garanzia dei restanti diritti naturali nella società civile, andrebbe declinato in chiave anti-entropica e in funzione della prosperità degli enti informazionali e di tutta l'infosfera. Nel caso del contrattualismo di Rousseau, la natura "generale" della volontà espressa democraticamente in assemblea andrebbe accordata ai medesimi criteri offerti dall'arricchimento delle proprietà informative del sistema.

Tuttavia, a differenza di Dworkin, l'intento non è di riprendere gli assunti della teoria di Floridi per rinverdire la speranza di ottenere un'"unica risposta corretta". Infatti, anche a seguire le quattro leggi morali, finiremmo per incontrare, prima o poi, alcuni bivi o diramazioni nell'argomentazione giuridica, per cui le difficoltà nelle quali va a parare di tanto in tanto l'ordinamento richiedono decisioni politiche, più che soluzioni di stretto diritto. La ragione riporta alla prima accezione di complessità esaminata nel capitolo secondo (v. § 2.1.3), dove si è sottolineato come le limitazioni che discendono dai fenomeni d'incompletezza nell'ambito matematico, valgano del pari per il linguaggio che ha di mira il mondo del diritto. Come riferito a proposito dell'approccio dell'"informativa e consenso" o del rapporto tra privacy e libertà di parola (§ 9.3.1), ci sono in fondo modi diversi per declinare il contrattualismo moderno in chiave anti-entropica o con l'arricchimento delle proprietà informative del sistema. Anche ad assumere le quattro leggi morali dell'etica dell'informazione come principi d'analisi, è per ciò indispensabile accoglierle con un certo margine di tolleranza, nel senso in cui l'espressione è comunemente usata nel linguaggio quotidiano; e cioè, allorché si ammette una qualsiasi differenza tra ciò che è stato progettato o fissato e la sua realizzazione effettiva, secondo lo scarto massimo ammissibile tra il valore nominale e quello reale di una determinata grandezza che funge da parametro, o punto di riferimento, come nel caso dell'entropia informativa.

Come illustrato in precedenza con la figura 28 di § 9.3, l'intento è di affinare su queste basi sia l'idea di ragionevolezza sottesa ai compromessi con cui, al modo di Hart, bisogna venire a capo dei casi difficili del diritto, sia l'aspettativa di privacy degli individui che si ritrovano davanti all'imprevedibilità degli scenari resi possibili dal progresso tecnologico. Ma, ancor prima di approfondire, sul piano normativo, la nozione di ragionevolezza sottesa ai casi difficili del diritto, conviene indugiare sul piano descrittivo dell'analisi con le nuove sfide che la tecnologia pone al diritto alla privacy e con la tutela dei dati personali. Si tratta dell'approccio che è già stato evidenziato in precedenti parti del libro, a proposito del passaggio dalle tradizionali forme di governo all'odierna governance (§ 3.3), oppure con i temi della nuova sorveglianza (§ 6.2.2), per cui occorre distinguere l'intento di cogliere il senso delle profonde trasformazioni in atto, dal prendere posizione di fronte a tali mutamenti, secondo il rapporto introdotto fin dal capitolo secondo (§ 2.1.2), tra IPR o Info2 (informazione per la realtà) e ISR o Info3 (informazione sulla realtà). Prima ancora di valutare le nuove sfide della privacy informazionale, in altri termini, è buona regola quella di comprendere preliminarmente il tenore di tali sfide.

A continuazione, queste sfide saranno illustrate con i casi concreti dei droni (§ 9.4.1), della robotica di servizio (§ 9.4.2), e con i nuovi ambienti "intelligenti" (§ 9.4.3). In questo modo, prestando attenzione alle proprietà del sistema e agli enti informazionali che lo compongono, potremo finalmente formalizzare il riposizionamento tecnologico del diritto in questo ambito dell'ordinamento, attraverso il test sulla ragionevole aspettativa (§ 10). Ma appunto, bisogna innanzitutto chiedersi cosa sia mai ragionevole attendersi in un mondo popolato da droni, robot domestici e cose che comunicano tra di loro in forma autonoma.

## 9.4. *Le nuove sfide tecnologiche*

Ci siamo più volte soffermati nel corso delle pagine precedenti sullo scopo che il diritto ha di governare la ricerca e lo sviluppo tecnologico (§ 1.1.3); sottolineando, altresì, come la tecnologia a sua volta incida sul diritto tanto dal punto di vista cognitivo, quanto degli istituti, tecniche e, in genere, delle istituzioni giuridiche (§ 1.4). Sul piano filosofico, è indubbio come questi due livelli dell'indagine siano strettamente connessi, quasi fossero due facce della stessa medaglia; sebbene, per ragioni di convenienza e chiarezza espositiva, si sia preferito talora di trattarli separatamente.

Nel sesto capitolo, introducendo i temi della privacy, si è così fatto riferimento al riposizionamento tecnologico occorso con le fotografie (§ 6.1.1), le banche dati (§ 6.1.2), e il web (§ 6.1.3), per introdurre l'esame della normativa rilevante ai fini della protezione dell'istituto, con i motivi dettati dal suo riposizionamento assicurativo (§ 6.2).

Nelle pagine successive, si è preferito invece insistere sull'intreccio d'innovazione tecnologica e intenti regolativi del diritto, per cui, nel capitolo settimo, ripercorrendo l'evoluzione della giurisprudenza della Corte suprema americana in tema di privacy e tutela del Quarto emendamento, si è analizzato come ai nuovi problemi posti dalla tecnologia del telefono (§ 7.2.1), dalle cabine telefoniche (§ 7.2.2), dalle camere fotografiche per aerei e satelliti (§ 7.2.4), fino ai sensori termici (§ 7.3.1), il GPS (§ 7.4), e gli smartphone (§ 7.5.2), la Corte di Washington abbia volta per volta deciso nei casi Olmstead, Katz, Kyllo, ecc. Nel capitolo ottavo, illustrando il sistema di garanzie del modello europeo per il trattamento dei dati personali, è stato del pari messo in evidenza il modo in cui il DNA e le tecniche d'identificazione biometrica (§ 8.2.3), gli strumenti d'analisi come il *profiling* o il *data mining* (§ 8.3.1), fino alle tecniche per l'anonimizzazione dei dati (§ 8.4), abbiano contribuito a loro volta all'evoluzione della normativa di riferimento.

In questa sede, occorre ora completare il quadro, prendendo in considerazione due ulteriori settori della ricerca scientifica e tecnologica, come la robotica e i programmi informatici volti alla realizzazione dei cosiddetti "ambienti intelligenti", le cui sfide alla tutela della privacy e dei dati personali sono destinate ad accrescere vistosamente nei prossimi anni.

Nel caso della robotica, si tratta di uno dei campi più dinamici e finanziariamente rilevanti della ricerca contemporanea, che comprende l'informatica e la cibernetica, la fisica e la matematica, l'elettronica e la meccanica, la biologia e le neuroscienze, fino ai vari settori delle scienze umane come la politica, la psicologia, l'economia o il diritto. Tra le varie applicazioni del ramo, è sufficiente menzionare i veicoli di terra come le macchine automatiche di Google, i droni e i robot militari come i MQ-9 *Reapers* e i C-3P0 *Terminators*, i robot da Vinci utilizzati nelle sale operatorie di urologia, fino alle applicazioni industriali che, dalla fine degli anni settanta del secolo scorso, hanno rivoluzionato per primo il settore automobilistico. Tale e tanta è la varietà, che spesso gli studiosi sono ancora divisi sulla definizione di ciò che è un robot: alcuni lo presentano come una macchina in grado di sentire, pensare e agire, secondo i dettami della ricerca contemporanea nell'ambito dell'intelligenza artificiale (Bekey 2005). Altri, come il direttore dei laboratori d'intelligenza artificia-

le all'università di Stanford, Sebastian Thrun, presentano i robot come macchine con l'abilità di "percepire qualcosa di complesso e di prendere le decisioni appropriate" (in Singer 2009: 77). Qui, conviene invece insistere come alcune di queste macchine siano, in realtà, dei veri e propri agenti artificiali, nel senso che, al pari degli esseri umani, anche gli agenti artificiali "agiscono". Riprendendo la tripartizione proposta da Allen, Varner e Zinser (2000), nel saggio sullo status degli agenti morali artificiali, si può dire che un ente – umano, animale o artificiale – "agisce" allorché esso sia interattivo, autonomo e capace di adattarsi al proprio ambiente. Questo in sostanza significa che:

a) l'agente risponde agli stimoli dell'ambiente attraverso il mutamento degli stati interni o valori delle sue proprietà (interattività);
b) l'agente è in grado di cambiare detti stati indipendentemente da stimoli esterni (autonomia);
c) l'agente è capace di accrescere o migliorare le regole attraverso cui tali stati cambiano (adattatività).

Su queste basi, il problema, oggi, non è tanto quello di determinare se e in che modo gli agenti artificiali e, in particolare, i robot eventualmente agiscano. Piuttosto, la questione verte sulla circostanza che l'interattività, autonomia e adattabilità dei robot comportano l'imprevedibilità delle loro azioni, sia nei confronti dei programmatori e costruttori di tali agenti artificiali sia dei loro stessi proprietari, per cui torna alla ribalta il problema di stabilire cosa sia mai "ragionevole" in questi casi (§ 9.3.2).

D'altra parte, nel caso della ricerca sugli "ambienti intelligenti" o "l'internet delle cose", il riferimento va a un variegato ambito scientifico e tecnologico che comprende sistemi d'identificazione tramite radio frequenza (RFID), reti neurali, sistemi multi-agenti e indagini biometriche di tipo comportamentale e, cioè, in grado di attribuire un preciso significato all'espressione del volto delle persone, al tono della loro voce, e via dicendo. Per rendere sin d'ora l'idea della posta in gioco, basta pensare a una scena di un film di fantascienza come *Minority Report* (2002), in cui il protagonista, Tom Cruise, mentre cammina per strada, è riconosciuto dall'interfaccia del muro di un edificio che comincia, per ciò stesso, a offrirgli pubblicità mirata. Ciò che ancora solo qualche anno fa pareva mera fantascienza, sta diventando rapidamente realtà, come avviene con la pubblicità personalizzata sulle pagine web d'internet o con Kinect, il gioco di Microsoft su piattaforma Windows Azure, che permette all'utente (umano) di interagire con la macchina usando la propria voce, o semplicemente gesticolando, mentre l'applicazione, grazie a una telecamera e a un microfono, è capace di raccogliere e processare i dati comportamentali dell'utente in tempo reale, al fine di profilarne le interazioni con quanto succede intanto nel video. Di qui ad applicare questo tipo di tecnologie al mondo reale – come già avviene in molti aeroporti del pianeta – il passo è breve. Quale aspettativa di privacy è dunque ragionevole attendersi in questi casi?

Sono tre le applicazioni con le quali saranno chiarite nel presente paragrafo, le nuove sfide della tecnologia: del variopinto mondo dei robot, innanzitutto, l'indagine si soffermerà su una classe popolare negli ambienti militari, i droni, che tuttavia cominciano a trovare svariate applicazioni anche nel settore civile (§ 9.4.1).

Dopo di che, considereremo un particolare tipo di applicazione domestica come la nuova generazione di robot badanti e di assistenti artificiali, più o meno scaltri, o intelligenti (§ 9.4.2).

Infine, prenderemo in rassegna l'insieme di tecniche utilizzate ai fini della creazione di "ambienti intelligenti" e per l'"internet delle cose" (§ 9.4.3).

Ciascuno dei tre casi serve a illustrare il nuovo riposizionamento della privacy con la protezione dei dati personali, precedentemente esaminati con il caso Katz (privacy in luogo pubblico: § 7.2.2), il caso Kyllo (privacy domestica: § 7.3.1), e il caso Jones (a spasso nell'infosfera: § 7.4).

L'obiettivo è di comprendere come sia destinato a mutare il significato del diritto alla privacy e in che senso gli ordinamenti debbano tenerne conto.

### 9.4.1. *La città dei guardroni*

Abbiamo riferito nel paragrafo precedente come la robotica militare sia uno degli ambiti della ricerca contemporanea più ricchi in finanziamenti: al suo interno, il settore della progettazione e produzione di RPAs (*remotely piloted aircrafts*), UAS (*unmanned aircraft systems*), oppure, più semplicemente, "droni", gode poi di particolare fortuna. Basti dire che uno studio di mercato del gruppo Teal ha stimato nel 2013 che gli investimenti raddoppieranno nei prossimi dieci anni, passando dagli odierni 5.2 miliardi di dollari spesi nel settore ogni anno, a 11.6 miliardi, per complessivi 89 miliardi di dollari nell'arco della decade. Per ciò che riguarda invece la distribuzione di tali investimenti nel mercato dei droni militari, un altro studio del gruppo di analisi e ricerca industriale HIS prevede che nel decennio 2011-2020, gli Stati Uniti investiranno il 56% della ricerca e sviluppo sui droni militari, la Cina il 12%, Israele il 9%, Russia l'8%, la ricerca pan-europea il 3%, e Regno Unito, Francia e Italia il 2% ciascuno. Come ricordato esaminando la legge di Moore (v. § 1.3), è significativo che, quando le truppe nordamericane invasero l'Iraq nel 2003, esse non disponessero di alcuna applicazione robotica. Per la fine del 2004, tuttavia, le unità erano diventate all'incirca 150, diventando 2400 l'anno dopo, e circa 12 mila prima del ritiro delle truppe da quel paese.

Come capitato già in altre occasioni con le ricerche militari [14], anche nel caso dei droni il loro uso si è man mano venuto estendendo al settore civile. Tra le varie applicazioni della tecnologia, è il caso dell'uso di droni per lo spegnimento degli incendi, il pattugliamento delle frontiere, il monitoraggio dell'ambiente e altro ancora. All'inizio del 2014, significativamente, sia la nota ditta Amazon sia Facebook hanno annunciato di pensare all'uso dei droni per recapitare i propri pacchi ai clienti e garantire una maggiore copertura globale per internet, rispettivamente. La corsa all'acquisto dei droni civili, che può farsi risalire al febbraio 2012, negli Stati Uniti, ha cominciato tuttavia a produrre i primi effetti indesiderati, come dimostra il caso di un ragazzo a Seattle, che ha pensato bene di entrare in possesso di un drone, con il

[14] Per molti versi l'esempio di scuola è rappresentato da internet, frutto della ricerca statunitense sul progetto ARPANET, sviluppato dall'agenzia del dipartimento della difesa di quel paese, DARPA, negli anni sessanta del secolo scorso (v. Ruffo 2012: 22).

quale spiare la propria ex fidanzata. Siccome, però, il Congresso di Washington ha da tempo fissato per il 2015, l'anno in cui lo spazio aereo dovrà essere aperto a questi velivoli, gli studiosi hanno cominciato a porsi il problema di come il loro uso debba essere disciplinato dalla legge e come la ragionevole aspettativa di privacy degli individui possa mutare di conseguenza.

Ad esempio negli Stati Uniti, stante la vocazione settoriale, si è fatto riferimento alla disciplina vigente in tema di intercettazioni, video-voyeurismo, leggi sui paparazzi e diritto di cronaca che, su scala prevalentemente statale, più che federale, regolano l'uso di fotografie, video o audio, potenzialmente intrusivi per la privacy (Kaminski 2013: 68). Tuttavia, non soltanto molte corti statunitensi si sono mostrate riluttanti a riconoscere una ragionevole aspettativa di privacy nei luoghi pubblici, come avviene nel caso dei droni (v. Danforth Zeronda 2010: 1138); ma, si è ammessa anche la peculiarità dei problemi giuridici posti dal loro uso, dato che si assommano in un'applicazione unica i problemi sollevati dalle tecniche dell'intercettazione, rintracciabilità delle persone e dei luoghi, video sorveglianza, cattura delle immagini e così via. Il risultato è che, negli Stati Uniti, sono state già presentati diversi disegni di legge, sia a livello statale, sia federale, al fine di vietare le fotografie fatte dai droni senza il consenso degli interessati, e di limitare l'uso di immagini e altre informazioni da parte dei civili [15].

In Europa, stante l'ispirazione garantista del modello a vocazione generale, le cose sembrano stare diversamente. Per quanto la raccolta, trattamento e uso dei dati personali sia compiuta dai droni in forma automatica e, in prospettiva, perfino autonoma, ci sarà pur sempre un responsabile (umano) per il trattamento di quei dati, sottoposto al consueto regime sulla qualità del trattamento: v. figura 24 di § 8.2.1. Inoltre, tale quadro di tutela è destinato a essere rafforzato dall'articolo 33 della proposta di regolamento che, come riferito più sopra (§ 9.2.2), stabilisce una "valutazione d'impatto sulla protezione dei dati […] quando il trattamento, per la sua natura, il suo oggetto o le sue finalità, presenta rischi specifici per i diritti e le libertà degli interessati". In particolare, sembrano entrare in gioco le garanzie della lettera (c) dell'articolo 33, che menziona espressamente "la sorveglianza di zone accessibili al pubblico […] mediante dispositivi ottico-elettronici (videosorveglianza) su larga scala".

Nondimeno, anche in Europa, ci sono due ragioni per cui l'impiego di questa tecnologia appare problematico e, comunque, destinato a mutare la percezione di privacy fin qui avuta dagli individui.

La prima ragione dipende dai limiti genetici del modello europeo (v. § 8.1.1), che possono essere qui approfonditi con il quadro di tutela messo a punto dall'ordinamento italiano. Per un verso, lo scenario di privati che spiino altri individui a mezzo di droni ricadrebbe semplicemente sotto la sfera di applicazione del vigente articolo 615 bis del codice penale – vale a dire le interferenze illecite nella vita privata delle persone – come del resto ribadito dalla Corte di cassazione l'8 marzo 2012. In quella occasione, un individuo è stato ritenuto colpevole di detto crimine "per

[15] Penso alla proposta di un *Texas Privacy Act* (H.B. 912 del 2013) e al *Preserving American Privacy Act* (H.R. 637 del 2013), rispettivamente.

essersi procurato, in qualità di esercente la professione di investigatore privato, mediante l'uso di strumenti di ripresa visiva e sonora, immagini e notizie della vita privata di K. T., riprendendo – mediante strumenti di registrazione – un rapporto sessuale tra la predetta e V. M., all'interno dell'abitazione di costui, cedendo poi il filmato al marito della donna, dal quale aveva ricevuto l'incarico di provarne l'infedeltà coniugale" [16]. Da questo punto di vista, per ciò, anche in Italia, in un caso come quello occorso all'ex fidanzata di Seattle, dovremmo stare al sicuro.

D'altro canto, però, le cose cambiano sensibilmente quando si consideri ciò che, nel gergo giuridico italiano, è definita la "videoripresa di immagini non comunicative". Secondo una lettura restrittiva delle garanzie previste all'articolo 14 della Costituzione, attinenti alla tutela del domicilio, non bisogna intenderne la nozione nel significato oggettivo del termine, mutuato dal diritto civile, e ripreso dall'articolo 614 del codice penale. Piuttosto, affinché scatti la tutela alla propria riservatezza, come dichiarato dalla Corte costituzionale nel 2008, occorre che l'individuo abbia un rapporto stabile con quel luogo e, soprattutto, che i suoi comportamenti nella dimora privata non siano visibili a terzi: "affinché scatti la protezione dell'art. 14 Cost., non basta che un certo comportamento venga tenuto in luoghi di privata dimora; ma occorre, altresì, che esso avvenga in condizioni tali da renderlo tendenzialmente non visibile a terzi" (sentenza 149 del 7 maggio 2008). Su queste basi, è intervenuta successivamente la Corte di cassazione in senso ancor più restrittivo, distinguendo la tutela costituzionale del domicilio dal diritto alla riservatezza fondato sull'articolo 2 della Costituzione, per cui la dignità kantiana delle persone, in sostanza, gode di un grado di tutela minore rispetto a quello accordato alla tutela del domicilio, delle comunicazioni e della libertà personale. Con le parole della Corte, "la tutela costituzionale del domicilio va tuttavia limitata ai luoghi con i quali la persona abbia un rapporto stabile, sicché, quando si tratti di tutelare solo la riservatezza, la prova atipica [una videoregistrazione, nel caso] può essere ammessa con provvedimento motivato dell'autorità giudiziaria. Non sono pertanto ammissibili riprese visive effettuate, ai fini del processo, in ambito domiciliare mentre vanno autorizzate dall'autorità giudiziaria procedente (p.m. o giudice) le riprese visive che, pur non comportando un'intrusione domiciliare, violino la riservatezza personale" [17].

Come ben si vede, la tutela approntata dall'ordinamento italiano non coincide affatto con l'ambito di tutela visto ai tempi del caso Jones (v. § 7.4): lì, la Corte suprema aveva dato ragione all'imputato, perché gli agenti federali lo "pedinarono" – sia pure tramite GPS – senza l'occorrente mandato di un giudice. In Italia, invece, si lascia "ampi ed incontrollabili poteri alle Procure" in quanto la "questione giuridica viene, infatti, surrettiziamente risolta ponendo l'accento sul diritto alla riservatezza, il quale, ricondotto negli stretti argini dell'art. 2 della Costituzione come espressione della dignità personale, non può godere delle garanzie della doppia riserva di legge e di giurisdizione", prevista invece dall'articolo 14 (v. Senor 2012). Al giorno d'oggi,

[16] Si v. Cass., sez. V penale, sentenza n. 9235: "l'investigatore privato che con la propria condotta insidia la riservatezza delle abitudini individuali o sociali (dunque dei rapporti umani) che in tali luoghi si svolgono, commette il reato di interferenze illecite nella vita privata punito dall'art. 615 bis c.p.".

[17] Cass., sez. VI penale, sentenza 33953 del 15 giugno 2012 (depositata il 3 settembre).

mentre si discute ancora accanitamente in Italia sul regime delle intercettazioni telefoniche o elettroniche, invece, si lasciano prive delle garanzie di un organo terzo e indipendente le videoriprese di immagini "non comunicative" e, cioè, esattamente quelle diventate popolari e d'uso comune negli Stati Uniti con l'impiego dei droni.

Potremmo naturalmente emendare il quadro di tutele costituzionali vigenti oggi in Italia, in modo da rendere il paese più simile al livello di protezione previsto in altri ordinamenti europei o, anche, solo allo standard di tutela definito dalla Corte suprema di Washington con il test sulla ragionevole aspettativa di privacy nel caso Jones.

Ma, pure a voler immaginare un'Italia giuridica più europea, oppure statunitense, c'è la seconda ragione per cui l'impiego dei droni è destinato a rimanere problematico. Anche ad ammettere che l'uso di questa tecnologia sia sempre e solo legale, nel senso forte dell'integrità della legge preconizzato da Dworkin (§ 9.3.1), il volo delle macchine robotiche autonome non può che incidere su ciò che è ragionevole attendersi sia tutelato in nome della privacy.

Basti riflettere sul modo in cui precedenti tecnologie abbiano già inciso sulla tutela della privacy nei luoghi pubblici, come occorso con l'uso di CCTV (§ 5.1.2), foto aeree (§ 7.2.4), e GPS (§ 7.4): la particolarità dei droni dipende precisamente dal fatto che tutti questi congegni e dispositivi tecnologici sono ora riassunti e impiegati da un'unica applicazione robotica. Tenuto conto degli innumerevoli impieghi socialmente utili di tali applicazioni, come nel caso della consegna dei pacchi a domicilio o al fine di sorvegliare come vadano le cose a casa vostra in campagna, assisteremo a un nuovo riposizionamento tecnologico dell'istituto e a nuove forme di bilanciamento tra visibilità delle persone e tutela della loro opacità. Basti per ora riferire come, fin dal 2013, siano disponibili negli Stati Uniti le applicazioni per *smartphone* che vi avvertono se per caso, dalle parti in cui vi trovate, ci sia in volo qualche drone.

### 9.4.2. *A casa nel 2045*

Abbiamo riportato nel capitolo primo (§ 1.2), la profezia di Ray Kurzweil, secondo cui i progressi dell'intelligenza artificiale e della robotica daranno vita a un'intelligenza di gran lunga superiore a quell'umana, da qui al 2045.

Tra gli addetti ai lavori, i termini della questione sono riassunti tradizionalmente con il test messo a punto, nel 1950, da un matematico a noi già noto, Alan Turing (v. §§ 1.4 e 2.1.1). Nel saggio *Computing machinery and intelligence*, Turing proponeva di venire a capo del problema se mai una macchina possa dirsi veramente intelligente, in ragione del test sull'interazione di un umano con un altro agente di cui, tuttavia, non se ne conosca la natura, umana o artificiale. Nel caso in cui l'essere umano non sia in grado di discernere la natura dell'ente con il quale interagisce, l'idea è che la macchina debba ritenersi a tutti gli effetti intelligente, avendo superato il test di Turing.

Senza entrare nel dibattito di questo ulteriore test, non c'è però bisogno di attendere una nuova generazione di robot intelligenti, al modo di Kurzweil, per ammettere, già da ora, che alcune di queste macchine, o agenti artificiali, hanno cominciato a incidere sulla privacy degli individui. Per chiarire il punto, converrà concentrarsi su un particolare tipo di applicazioni robotiche nel settore domestico, ossia i robot badanti e gli assistenti artificiali. Come ho cercato di spiegare in altre oc-

casioni (Pagallo 2013, 2013a), questi robot non sono macchine pronte per l'uso ma, al contrario, richiedono di essere allenate al fine di svolgere le funzioni per le quali sono state programmate; ovvero, esse devono essere per così dire allevate ed educate, né più né meno come occorre fare con un animale o un bambino. Quando, nel 2009, ispezionavo il robot NAO al convegno della Società britannica per lo studio dell'intelligenza artificiale e la simulazione del comportamento (AISB), a Edimburgo, rimasi colpito dal modo in cui i costruttori di NAO dovevano insegnare all'umanoide come usare il proprio corpo, alto 57 centimetri, insieme al software di cui è equipaggiato, per muoversi, camminare, ballare e interagire con gli esseri umani o altri robot. L'anno dopo, alla nuova conferenza AISB a Leicester, nella primavera 2010, confesso di essere rimasto impressionato dai progressi nel frattempo fatti da NAO, e da quanto bravo fosse diventato a suonare addirittura il violino!

Una particolarità di questa classe di robot concerne pertanto il modo in cui il loro comportamento dipenda da come gli individui allenino, curino o trattino le macchine. Nell'ambito della ricerca scientifica, gli studi nell'ambito dell'interazione uomo/robot (HRI: da *human/robot interaction*) suggeriscono alcuni dei parametri cui occorre fare caso: i diversi tipi di contatto con gli uomini, le funzioni e ruoli dei robot, nonché le loro abilità sociali nell'interagire con gli altri. Più in particolar modo, all'interno della ricerca HRI, si distingue un approccio imperniato sulle aspettative umane e uno, invece, imperniato su quelle dell'agente artificiale. Nel primo caso, l'idea è di creare robot che agiscano entro i limiti che gli esseri umani possano accettare in termini razionali: "l'HRI centrato sull'uomo è fondamentalmente interessato a come un robot possa adempiere alla specificazione dei suoi compiti, in maniera da essere accettabile e confortevole per gli umani" (Dautenhahn 2007: 684). Nel caso dell'approccio HRI imperniato sulle attese del robot, si discorre viceversa del "paradigma del badante", ossia gli umani come badanti dei propri robot. Benché i "bisogni sociali" dell'agente artificiale siano stabiliti dal design della macchina – e modellati dall'architettura interna di controllo del robot – sono pur sempre gli utenti che permettono al robot di sopravvivere al proprio ambiente, venendo incontro ai propri bisogni. Una ricerca antesignana su Kismet, ossia una testa robotica con funzionalità di tipo sociale, mostra come abbia proceduto questo tipo di ricerca (Breazeal 2002): la macchina viene trattata come un'entità autonoma, che persegue i propri fini in ragione delle sue stesse motivazioni, per cui il partner umano è chiamato a soddisfarne gli impulsi sociali, individuando e rispondendo ai bisogni interni della macchina.

La morale da trarre da questo tipo di applicazioni è duplice. Per un verso, sul piano della responsabilità giuridica, un nuovo tipo di responsabilità per fatto altrui verrà a formarsi, avendo a che fare con un comportamento che non è né certamente umano, né animale, bensì, "intelligente artificiale". Per quanto si ricorra all'analogia con i consueti casi di responsabilità oggettiva per le malefatte dei propri animali, bambini o dipendenti (v. § 8.5), la peculiare imprevedibilità dei robot, poggiante in parte sostanziale sulle tecniche informatiche per l'apprendimento delle macchine, o *machine learning*, ha già creato una serie di problemi inediti nel decidere chi risponda per un'azione determinata e il danno conseguente (v. Pagallo 2013: 119-132).

D'altra parte, interagendo con gli uomini nella sfera domestica, i robot sapranno molte cose su chi vive in quelle case: a partire dagli anni dieci la ricerca robotica ha inoltre puntato sulla connessione in rete di questi agenti artificiali, per facilitare

compiti di posizionamento con GPS e Google Maps, accrescimento o scambio delle informazioni tramite l'accesso a internet, o per inferire conclusioni da dati statistici, sulla cui base prendere poi decisioni al posto vostro: prenotazioni di alberghi, noleggio delle macchine, visite dentistiche, ecc. Gran parte di queste informazioni, va da sé, saranno informazioni e dati personali, per non dire "sensibili" (§ 8.2.3). Per venire a capo di questi problemi, al ricordato incontro dell'AISB a Edimburgo, ne discutevo con la squadra di lavoro dell'Aldebaran – la ditta costruttrice di NAO – ponendo loro il problema di cosa potesse capitare ai miei dati personali, nel caso in cui NAO fosse stato per caso sequestrato. I tecnici dell'Aldebaran spiegavano che, in situazioni estreme, si può staccare la memoria di NAO in remoto, come del resto avviene con l'iPhone in caso di furto. Altre forme, anche più sofisticate, di protezione dei dati personali sono state proposte nel frattempo nel settore, più volte menzionato, della "privacy tramite design" (§ 9.2.5).

Ma, anche a lasciare in parentesi la questione d'immettere nella memoria di NAO l'insieme di regole e principi per la protezione dei dati che la Commissione ha proposto nel nuovo regolamento, rimane aperto un ulteriore problema. Il fatto che i robot domestici diventino progressivamente dei veri e propri agenti – e cioè esseri interattivi, adattativi e autonomi – non potrà infatti che incidere sulla ragionevole aspettativa che le persone avranno sulla tutela della propria privacy. A seconda del tipo di robot con cui avremo a che fare, nuovi livelli di accesso e controllo sulle informazioni e dati personali andranno tarati nelle case delle persone, come avviene, del resto, quando vi fa visita un amico, un parente, un semplice conoscente o la portinaia, e di qui, in ragione del contesto, modulate il livello di riservatezza che vi sembra opportuno. L'entrata in scena di una nuova generazione di robot domestici trasforma il consueto scenario della doppia aspettativa tra individui – "io mi aspetto che tu ti aspetti…" – con l'interazione, anche affettiva, con un programma. Molti lettori avranno forse visto il film che, nel 2013, ha reso popolari questi temi con le avventure di un nuovo sistema operativo particolarmente intelligente, "Lei" (*Her*). Bisognerebbe, però, aggiungere che, insieme ai dispositivi militari, uno dei settori, da sempre, più corteggiati nel campo della robotica, riguarda la robotica sessuale: tra le centinaia di articoli e volumi al riguardo, mi limito a segnalare *Love and Sex with the Robots* di David Levy (2007). Già nel febbraio 2008, in fondo, è significativo che l'autorevolissimo mensile *Scientific American* abbia ospitato il dibattito, in alcuni ambienti perfino acceso, su possibili matrimoni misti tra robot e umani. Quale ragionevole aspettativa di privacy potremo avere nelle nostre case?

### 9.4.3. *Onlife*

L'espressione "onlife" va innanzitutto riferita a un progetto della Commissione europea, nel quadro generale del programma sui "futuri digitali", che da un punto di vista inter, o trans, disciplinare ha inteso indagare come la quarta rivoluzione incida sulla condizione umana, modificando il rapporto che gli uomini hanno con se stessi, con gli altri e con il mondo in generale. Con le parole del documento finale (*Onlife Manifesto*, a cura di Luciano Floridi 2014), "l''incessante espandersi delle ICT scuote alle fondamenta i tradizionali quadri di riferimento concettuali attraverso le seguenti trasformazioni:

a) l'erosione dei confini tra il reale e il virtuale;
b) l'erosione dei confini tra uomo, macchina, e natura;
c) il rovesciamento della situazione nella sfera dell'informazione: dalla scarsità alla sovrabbondanza;
d) la transizione dal primato del soggetto al primato dell'interazione".

In questa sede, la trasformazione in corso relativamente alla condizione umana va parametrata al modo in cui la privacy degli individui sta mutando sia nei luoghi pubblici, sia a casa propria, sia in quello spazio dell'infosfera che, prima (§ 9.4), si è introdotto con la formula degli "ambienti intelligenti" e l'"internet delle cose". Si tratta di uno dei settori più frequentati dagli odierni studi sulla tutela dei dati personali, dato che la progettazione di questi ambienti che profilano o anticipano le scelte e i comportamenti delle persone, solleva molteplici rischi per la tutela della privacy con nuove e anche sofisticate forme di discriminazione; come quando, ad esempio, non viene concesso un credito per via delle indagini statistiche di una data multinazionale del settore. La dinamica della doppia aspettativa tra individui – "io mi aspetto che tu ti aspetti…" – messa in mora dallo sviluppo dei robot, torna in primo piano con gli scenari degli ambienti intelligenti e l'internet delle cose, per un duplice ordine di ragioni. Da un lato, la profilazione delle persone può anche essere corretta e, però, gli individui, ignari della profilazione, si trovano nella condizione di non poterne contestare la rilevanza: è la situazione in cui ci potremo trovare quando incontreremo non solo NAO, ma pure simili modelli di nostri conoscenti e amici. D'altro canto, se la profilazione fosse anche imperfetta, l'individuo potrebbe reagire ai responsi dell'ambiente cambiando il proprio comportamento che, a sua volta, potrà rafforzare i termini della profilazione secondo il canone della profezia che si auto-avvera.

Il modo consueto in cui gli ordinamenti hanno provveduto a correre ai ripari, come si è visto, è dato dalle forme del diritto all'accesso (§§ 8.2.2 e 8.2.4).

Tuttavia, è stato convincentemente argomentato per quale ragione non sia bene illudersi che l'esercizio del diritto all'accesso sia la chiave con cui risolvere i problemi di privacy posti dallo sviluppo degli "ambienti intelligenti"; se mai, bisognerebbe pensare a nuove forme di "giusto processo" con cui aggiornare la giurisprudenza della Corte europea dei diritti dell'uomo sull'articolo 6 della Convenzione, stante la quale occorre garantire che le parti in causa giochino, per così dire, "ad armi pari" (Hildebrandt 2011).

Inoltre, riprendendo temi e motivi studiati con le diverse modalità del design (§§ 5.2 e 5.3), bisogna prestare attenzione al ruolo che le infrastrutture ICT – che rendono gli ambienti intelligenti fattibili – svolgono come agenti regolativi del sistema: un algoritmo invisibile "predirà salute e altri rischi, calcolerà le nostre capacità educative, occupazionali o professionali, misurerà la nostra resistenza allo stress e all'esaurimento, predirà la probabilità di un comportamento violento o di condotte criminali, permettendo all'ambiente intelligente di includere o escludere con discrezione da certi servizi, prodotti, assicurazioni, locazioni, opportunità educative o professionali, consentendo altresì all'ambiente intelligente di proibire o dare accesso ad ambiti fisici o online. Si noti ancora che l'infrastruttura computazionale non forzerà gli ambienti intelligenti ad agire in un modo preciso; non c'è nulla di deterministico

qui. Ma sarebbe da ingenui non riconoscere che queste possibilità cambiano la terra sotto i piedi […] chiedendoci di ristallare un sistema di pesi e contrappesi [*check and balances*] per opporsi agli effetti indesiderati" (Hildebrandt 2011).

Il problema di quale possa essere la nostra ragionevole aspettativa di privacy in questi ambienti, in cui le cose comunicano tra di loro, i robot provvedono ai nostri affari, o i droni volano, impercettibili, per la città come già nel film *Blade Runner*, suggerisce di tornare ai presupposti filosofici di cosa debba intendersi per "ragionevole" nell'era della quarta rivoluzione (§ 9.3.3). In precedenza, richiamando le quattro leggi morali dell'etica dell'informazione di Floridi, si è accennato ai diversi modi in cui è possibile declinare il contrattualismo moderno in chiave anti-entropica o con l'arricchimento delle proprietà informative del sistema. Qui, l'idea può essere approfondita, rappresentando gli enti onlife come un insieme discreto e unitario di dati, aventi le appropriate strutture e dotati dell'insieme delle operazioni, funzioni e procedure che qualificano, nella sua individualità, ogni ente informazionale. A questo livello di astrazione, possiamo decodificare il plesso di principi, regole, decisioni e pratiche che caratterizzano il diritto alla privacy e la tutela dei dati personali, come forze che si oppongono al flusso delle informazioni negli ambienti intelligenti. Si tratta di ciò che Floridi definisce altrimenti come la "frizione ontologica" nell'infosfera, vale a dire "l'ammontare di lavoro e sforzi richiesto a un certo agente per ottenere, filtrare e/o bloccare informazione (pure, ma non soltanto) su altri agenti in un ambiente determinato" (Floridi 2006: 4). La tutela della privacy informazionale degli individui corrisponde in questo modo all'obiettivo di mantenere l'integrità di quel pacchetto discreto e ben strutturato di dati, secondo cui è possibile intendere la stessa identità degli individui. Sulla base dei "gradi di frizione" che è dato calibrare nell'infosfera, occorre per ciò mantenere ferme le distinzioni tra agenti e sistema, individui e società, secondo il meccanismo per cui, maggiore la frizione ontologica in una data regione dell'infosfera, minore l'accessibilità all'informazione personale sugli agenti e, pertanto, maggiore la protezione della loro privacy informazionale. Il susseguirsi di leggi e di sentenze in tema di privacy, nel corso dei capitoli precedenti, può essere interpretato come la disciplina dei diversi gradi di frizione ontologica che gli ordinamenti sono venuti riconoscendo a tutela delle persone.

Abbiamo tuttavia detto che, per via della complessità informazionale del nostro tema, non si può dedurre dalle leggi morali dell'etica dell'informazione un criterio unico, sulla cui base offrire la "risposta corretta" a tutti i problemi aperti della privacy (§ 9.3.3). Ciò nondimeno, quest'ultima prospettiva suggerisce il modo di giudicare gli odierni sforzi, e del gubernaculum e della iurisdictio, relativi ai "gradi di frizione ontologica" che occorre mantenere in funzione anti-entropica o per la ricchezza informativa degli enti e degli ambienti intelligenti. Si tratta di badare al significato del termine che qualifica fin dall'inizio il test messo a punto dal giudice Harlan: la ragionevolezza. Bisogna in sostanza riflettere sull'attuale quadro normativo, pensando alle sfide che la tecnologia pone e che, fino a poco tempo fa, potevano sembrare semplicemente fantascientifiche. Le questioni destinate a sorgere con droni, robot domestici e negli ambienti intelligenti, suggeriscono infatti un nuovo riposizionamento tecnologico dell'istituto; benché, per molti versi, molto più radicale di quanto occorso con precedenti innovazioni tecniche – in fondo, abbiamo a che fare ora con nuove forme di intelligenza artificiale.

Declinato in chiave di ragionevolezza informativa, il test ha di qui una duplice funzione: non solo quella di valutare l'odierno stato dell'arte per prendere posizione rispetto ai problemi, odierni e futuri, della privacy; ma, anche per chiedersi cosa sia ragionevole attendersi in uno spazio condiviso con droni (luoghi pubblici), robot (domestici), e tra cose che comunicano fra sé (onlife).

Su questo duplice tema s'incentra il capitolo conclusivo del libro.

# X.
# *Test*

> "Se è vero che c'è sempre più di un modo per costruire un testo, non è vero che tutte le interpretazioni si equivalgono"
>
> Paul RICOEUR

La nozione di test, su cui siamo venuti discorrendo nei capitoli precedenti, sia a proposito del caso Katz (§ 7.2.2), sia di Kant (§ 5.3.3.1), o di Simon (§ 1.4.1), o di Turing (§ 9.4.2), o di Kelsen (§ 4.1), deve essere approfondita secondo un duplice punto di vista. Il riferimento va a ciò che i filosofi medioevali definivano come *genus proximum* e *differentia specifica*; vale a dire, rispettivamente, quanto accomuna e diversifica i vari test con cui possiamo essere alle prese: il test d'intelligenza, il test attitudinale, il test di gravidanza, ecc.

Per un verso, sul piano dell'identità, ogni test si profila secondo un significato eminentemente operativo, come un esperimento o prova, sulla cui base vagliare l'oggetto del test medesimo; è il caso della ragionevole aspettativa di privacy nel caso Katz, della legittimità di ogni legge pubblica nel caso del contratto sociale di Kant, della possibilità di scomporre la ricerca scientifica in blocchi operativi per Simon, dell'intelligenza di un ente artificiale nel caso di Turing, della doppia condizione di validità delle norme in Kelsen, e così via.

D'altro canto, sul fronte della differenza specifica, occorre badare al tipo d'informazione che si mira a ottenere con il test. Riprendendo le distinzioni del capitolo secondo (§ 2.1), bisogna così distinguere l'informazione sulla realtà da quella per la realtà. Nel primo caso, si ha a che fare con un'informazione di tipo semantico che informa sui diversi stati del mondo e, come tale, risulta qualificabile come vera o falsa: è ad esempio la prova del test di gravidanza. Nel secondo caso, abbiamo piuttosto a che fare con un insieme di regole o istruzioni che determinano il modo di essere di altre entità: questo è il caso più frequente nell'ambito dei test giuridici, come quello di Katz o di Kant, o di Kelsen.

Tuttavia, come riferito sempre nel capitolo secondo, nulla esclude che alcuni di questi test, come nel caso Katz, possano essere convenientemente impiegati anche per stabilire l'attendibilità dei risultati ottenuti tramite rilevazioni statistiche per campioni: è il diverso punto di vista che separa, poniamo, il normativismo giuridico da certe forme di realismo e dalla sociologia giuridica.

Sulla scorta dell'analisi svolta nelle pagine precedenti, conviene nondimeno insistere sul profilo normativo del test sul fronte giuridico, ossia il tipo d'informazione

di cui abbiamo bisogno per stabilire se l'aspettativa di privacy sia ragionevole e vada pertanto tutelata o, per dirla ancora con Kant, se la normativa del legislatore possa derivare dalla volontà comune di tutto un popolo. Più in particolar modo, concentrando l'attenzione sui profili normativi del test messo a punto dal giudice Harlan nel caso Katz, occorre metterne in evidenza tre aspetti che, sia pure emersi nel corso delle pagine precedenti, vengono qui riepilogati per comodità espositiva.

Il primo punto riguarda l'ordinamento in cui il test sulla ragionevole aspettativa di privacy è nato, quello degli Stati Uniti d'America, con i problemi cui esso è andato incontro, da ultimo, con il caso Jones (§ 7.4.1). Il tradizionale punto di forza del test e, cioè, con le parole di *justice* Harlan, il richiamo a una aspettativa "tale che la società sia pronta a riconoscere come ragionevole", può infatti diventare il suo tallone d'Achille in epoche di "drammatico mutamento tecnologico […] in cui le aspettative popolari sono in flusso", per dirla questa volta con l'opinione di *justice* Alito (§ 7.4.1.1). Secondo il parere condiviso da Sonia Sotomayor, il riposizionamento tecnologico dell'istituto ben può innescare un gioco al ribasso, stante il quale gli individui finiscono per essere disposti ad accettare un minor grado di tutela in cambio di più servizi, o di maggiore sicurezza; e comunque, a giudizio di *justice* Sotomayor, sarebbe il caso che la Corte rivedesse finalmente il proprio tradizionale orientamento che individua nella segretezza il prerequisito di tutela ai sensi del Quarto emendamento, declinando la privacy come limitazione. Lasciando da parte gli ulteriori problemi inerenti alla circolarità del test e al rischio che, in nome di quest'ultimo, i giudici possano legittimare qualsivoglia decisione essi assumano, tornano alla mente le parole di Barry Steinhardt, per cui "non dobbiamo chiedere all'Europa di adeguarsi al nostro modello, ma piuttosto noi adeguarci al loro" (§ 7.5.2). L'idea che la segretezza sia un prerequisito di tutela della privacy, in fondo, è stata da tempo screditata nel vecchio continente; e, del resto, anche la tesi di Alito sulla centralità delle scelte legislative è stata da sempre il fulcro del modello europeo.

Passando al secondo aspetto suggerito dai profili normativi del test, c'è tuttavia da dire che anche il modello del vecchio continente incontra i suoi problemi, stante l'abbondanza di disposizioni e vincoli che il legislatore europeo è venuto introducendo per definire le condizioni di legittimità per il trattamento e uso dei dati personali (§ 9.2.2). Anche ad ammettere, con il tipico approccio "dall'alto verso il basso" del legislatore di Bruxelles, che quest'ultimo sia sempre in grado d'individuare l'opportuno bilanciamento tra i diritti e gli interessi in gioco, rimane il fatto che non solo i cittadini europei, ma gli stessi esperti, trovano spesso difficoltà a orientarsi nella fitta rete di disposizioni comunitarie, normative nazionali, opinioni e raccomandazioni delle autorità, o precedenti delle corti. Basti far cenno, ancora una volta, ai dilemmi del consenso degli interessati (§§ 8.3.1 e 9.2.2), ai limiti del riuso (§ 8.4), alle scelte legislative in tema di cancellazione dei dati in rapporto ad altri diritti, come la libertà di parola (§ 9.2.3), o ai poteri esecutivi di un organo non rappresentativo come la Commissione (§ 9.2.4). Come si è ricordato più sopra, il rischio in questo caso è di fare dei dati, sia pure personali, un feticcio, smarrendo per strada quanto *justice* Harlan riassumeva con l'aspettativa che l'individuo ha di vedersi protetto nei confronti di forme aggressive di sorveglianza elettronica e, cioè, a tutela della propria privacy.

L'ultimo profilo normativo del test ha infine a che fare, sia negli Stati Uniti che

in Europa, con la nozione di ragionevolezza (§ 9.3.3). Tanto dal punto di vista del profilo oggettivo messo a punto da *justice* Harlan con il suo test, quanto dalla prospettiva delle scelte legislative maturate nel modello europeo, occorre fare i conti con la natura stessa dell'istituto che, ora sul fronte delle scelte individuali, ora su quello delle decisioni politiche, appare irriducibile a una logica del tutto o niente ma, al contrario, propone più spesso questioni di ragionevole bilanciamento (§§ 6.2.2, 8.4, 9.2.3, ecc.). A ben vedere, se non sono mancati gli esempi di un intervento poco ragionevole da parte del legislatore, il profilo normativo evocato dal test appare tanto più urgente, quanto più si sia consapevoli del nuovo riposizionamento tecnologico dell'istituto (§§ 9.4-9.4.3). Si tratta di ciò che, sulla scorta dell'etica dell'informazione di Floridi, abbiamo cominciato a rappresentare come gradi di "frizione ontologica" nell'infosfera, al fine di chiederci cosa sia ragionevole attendersi in un mondo popolato da droni, robot domestici, o da cose che comunicano tra di loro in forma autonoma.

Al fine di orientarsi innanzi a questo insieme di problemi, quest'ultimo capitolo è suddiviso in cinque paragrafi; nel primo dei quali (§ 10.1), sarà utile circoscrivere l'ambito dell'indagine all'insegna della nozione di "privacy informazionale". Mentre, infatti, è dato concepire la tutela della privacy prescindendo dalla protezione dei dati personali (privacy tradizionale) o, viceversa, quest'ultima senza privacy (il feticcio dei dati), l'attenzione andrà rivolta, sia sul piano descrittivo sia normativo, all'ambito dove i due settori convergono o si sovrappongono.

Su queste basi, passeremo brevemente in rassegna l'idea di "trapianto giuridico" (§ 10.2). Secondo il neologismo coniato negli anni settanta dal giurista scozzese Alan Watson (n. 1933), l'intento è di circoscrivere ulteriormente l'indagine sul modo in cui il test nordamericano sulla ragionevole aspettativa di privacy possa essere proficuamente impiegato anche nel modello giuridico europeo della privacy informazionale. Più che trapiantare il test in quanto tale, si mirerà a impiegarlo come banco di prova critico.

Questa prospettiva sarà sviluppata nel prosieguo del capitolo, per segnalare come, sia che si aspiri a criticare la legislazione europea vigente, sia che si ambisca a delineare i prolegomeni a ogni legislazione futura, è necessario fondare in termini filosofici la nozione di ragionevolezza (§ 10.3). Mentre, nel capitolo precedente, questa prospettiva è servita a introdurre i termini e modi del nuovo riposizionamento tecnologico della privacy informazionale, qui si tratterà invece di approfondire il senso in cui va declinata la tolleranza del test sulla ragionevole aspettativa di privacy.

Infatti, esistono quattro modi secondo cui questa tolleranza può essere intesa: ora riconducendola all'ideale di giustizia, ora intendendola in senso autonomo, ora come esito dell'insufficienza della giustizia intesa quale unico parametro per affrontare la complessità dei problemi in gioco, ora infine come grado ragionevole d'indeterminatezza (§ 10.4). Nel circoscrivere una volta di più lo spettro dell'analisi sulla base di quest'ultima nozione della tolleranza del test, bisognerà prestare attenzione al diritto come pratica sociale e a ciò che possiamo apprendere dalla interazione degli individui, secondo l'impostazione originaria dei profili soggettivi e oggettivi del test di Harlan.

A conclusione del capitolo (§ 10.5), sarà giunta l'ora di mettere alla prova il test con la dose d'umiltà che i fenomeni giuridici d'incompletezza in fondo suggerisco-

no. Circoscritta l'indagine con la nozione di privacy informazionale e facendo uso del test come banco di prova critico, la ragionevole tolleranza che dipende dalla complessità del fenomeno giuridico consiglia di fare attenzione ai rischi dell'uso dei dati personali, senza fare per ciò della cura di tali dati un feticcio.

## 10.1. *Privacy informazionale*

Nell'introduzione al capitolo ottavo, abbiamo evidenziato le tre caratteristiche peculiari che contraddistinguono il regime di protezione dei dati personali rispetto alla tradizionale tutela della privacy. In primo luogo, si è fatto riferimento ai dati, piuttosto che alle informazioni degli individui; poi, al bene giuridico che si mira a proteggere, sulla base della trasparenza del processo di raccolta e trattamento di quei dati, con i conseguenti obblighi di fare in capo ai responsabili e incaricati del trattamento; per giungere alla opposizione con lo stato o condizione di opacità delle persone – ossia, al loro non dover essere del tutto trasparenti agli altri – che abbiamo ripreso dall'opera di Hannah Arendt.

Su queste basi, è dato ora rappresentare la relazione tra il tradizionale diritto alla privacy, risalente all'opera di Warren e Brandeis (§ 6.1), e il diritto alla protezione dei dati, in ragione di tre ipotesi diverse:

i) innanzitutto, il diritto alla privacy può concepirsi in forma autonoma rispetto alla disciplina giuridica dei dati personali, secondo quanto suggerisce la distinzione tra gli articoli 7 e 8 della Carta UE dei diritti fondamentali (v. § 8.1). Analogo discorso, va da sé, vale nel sistema giuridico statunitense con i casi di tutela della privacy contro forme di appropriazione indebita, intrusione, diffusione di fatti privati o loro distorsione sotto "falsa luce", che non sollevano necessariamente problemi di raccolta o trattamento di dati personali (v. §§ 6.3.3 e 7);

ii) viceversa, la disciplina giuridica dei dati personali può presentarsi sganciata dalla protezione individuale della privacy: tra i numerosi esempi della vigente legislazione europea, è il caso di ricordare alcuni eccessi nella protezione dei cosiddetti dati sensibili (§ 8.1.3), o nel riuso dei dati (§ 8.4). Tra ciò che bolle in pentola con il nuovo regolamento europeo, è sufficiente invece ricordare l'esempio del cosiddetto diritto all'oblio e il diritto alla cancellazione dei dati (§ 9.2.3);

iii) infine, ci riferiamo alle ipotesi in cui la tutela della privacy e quella dei dati personali si sovrappongono, nel senso che la trasparenza con la quale i dati sono raccolti, trattati e impiegati nell'intero ciclo vitale dell'informazione, risulta funzionale alla tutela dell'"opacità" degli individui. In questo senso, si parla propriamente di privacy informazionale, essendo l'obiettivo quello di tutelare l'integrità di quell'insieme discreto e ben strutturato di dati, secondo cui l'identità degli individui può essere adeguatamente rappresentata, alla luce dei gradi di "frizione ontologica" tra agente e sistema, individuo e società (§ 9.4.3).

Avendo presente il disegno del presente capitolo, e cioè di estendere al modello europeo il test sviluppato dalla Corte suprema americana sulla scia dell'opinione concorrente di *justice* Harlan nel caso Katz, possiamo lasciare da parte la prima delle tre ipotesi ora menzionate, per concentrarci sulla seconda, con i possibili rischi di

rendere la tutela dei dati personali un feticcio; e, soprattutto, sulla terza ipotesi, in cui questa tutela appare funzionale alla protezione della privacy informazionale degli individui.

Dal punto di vista metodologico, l'applicabilità del test di Harlan alla protezione dei dati in Europa richiede nondimeno un'apposita digressione, alla luce di ciò che più spesso nel campo degli studi di diritto comparato, dagli anni settanta dello scorso secolo, si è cominciato a definire come "trapianto giuridico". Definito, nel prossimo paragrafo, cosa possa intendersi con quest'ultima formula, e come essa venga declinata in questo contesto (§ 10.2), sarà possibile proseguire l'indagine sull'"esportazione del test" (§ 10.3).

## 10.2. *Trapianti giuridici*

Le assonanze e parallelismi tra medicina e diritto sono tanto antichi, quanto la stessa tradizione giuridica e politica occidentale. A ben pensarci, parliamo tuttora, indifferentemente, di "costituzione", per indicare sia la legge giuridica fondamentale di una determinata comunità politica (§ 3.1.3), sia il modo d'essere secondo cui una persona fisica è costituita o composta: la sana e robusta costituzione di un individuo. Risalente fin dai tempi dell'antica cosmogonia greca e, cioè, dai miti fondativi e dai poemi sull'origine e formazione dell'universo, il parallelismo può essere illustrato con un'opera a noi già nota, la *Repubblica* di Platone (§ 1.1). Poco prima di cominciare a spiegare a Glaucone come nasca uno stato – secondo l'argomentazione del dialogo, riportata sopra nel capitolo primo – Socrate motiva infatti la necessità di "costruire a parole uno stato fin dalla sua origine" sulla scorta del parallelismo tra stato e individuo. Dovendo, nel secondo libro della *Repubblica*, spiegare in cosa consista la giustizia, la digressione che Socrate fa a proposito della formazione dello stato si giustifica così, in ragione del fatto che lo stato è un individuo scritto a lettere maiuscole: "Ebbene, in un àmbito maggiore ci sarà forse più giustizia e la si noterà più facilmente. Perciò, se volete, cerchiamo prima negli stati che cosa essa sia. Esaminiamola poi con questo metodo anche in ogni individuo e cerchiamo di cogliere nelle caratteristiche del minore la somiglianza del maggiore" (368e-369a, p. 76).

Esiste tuttavia un'ulteriore ragione per spiegare perché, quando Alan Watson conia nel 1974 il termine "trapianto giuridico", la formula non solo non sia apparsa bizzarra o impropria; ma, piuttosto, l'ingresso di un nuovo termine medico in ambito giuridico abbia riscosso tanta fortuna. Come è emerso a più riprese nel corso del libro, a proposito del pluralismo medioevale (§ 4.2.1), oppure delle corti costituzionali (§ 3.2.1), i trapianti giuridici sono in fondo tanto antichi, quanto il codice Hammurabi risalente al diciassettesimo secolo a.C. (Watson 1974: 27). Oltre all'originario parallelismo tra medicina e diritto, la fortuna della formula di Watson è dipesa dal fatto che veniva coniato un nuovo termine per ciò che, in sostanza, è esistito "da sempre". Secondo la tesi del giurista scozzese, si può anzi dire che il prendere a prestito istituzioni, concetti o strutture giuridiche, è da annoverare tra i fattori più fruttuosi o fertili dello sviluppo e delle dinamiche del diritto. Sebbene, come diremo, non siano mancate "crisi di rigetto", è altrettanto vero che molte operazioni di trapianto sono invece state coronate dal successo. Nell'accingerci a vagliare il

modello europeo della privacy informazionale con un test maturato in un altro sistema giuridico, vale dunque la pena di soffermarci sulla doppia possibilità che è congenita a ogni trapianto. Alla luce delle differenze, anche notevoli, che siamo venuti appurando nel corso della seconda parte di queste pagine tra Stati Uniti ed Europa, possiamo infatti trarre ispirazione, e cautela, prima di provvedere all'esportazione del test.

### 10.2.1. *Crisi di rigetto*

Al pari del mondo della medicina, anche nel mondo giuridico non tutti i trapianti sono possibili o, quantomeno, possono provocare crisi di rigetto. Nel caso specifico della privacy, ho avuto modo di occuparmene a suo tempo, a proposito della tutela dell'istituto in Giappone (v. Pagallo 2008: 46-49). Forse per le affinità elettive del lontano Oriente con il campo dell'elettronica e, in genere, della tecnologia, è significativo che questo paese sia stato fra i primi ad aver adottato una legislazione per la protezione dei dati personali processati da organismi amministrativi a mezzo di computer (la legge 95 del 16 dicembre 1988); cui ha fatto séguito, il 1° aprile 2005, la prima disciplina generale per la protezione dei dati e informazioni personali varata dal governo. Mancando una specifica parola nella lingua tradizionale, il termine è stato reso nel modo in cui i giapponesi pronunciano il vocabolo straniero, per cui, reso con il sillabario fonetico impiegato specialmente per questo tipo di parole, lo *katakana*, l'espressione di privacy è entrata a far parte del lessico giapponese moderno con il termine di *puraibashii*. Stante l'interpretazione formalistica e a tratti tipicamente zelante della nuova legge, imperniata su criteri individualistici che male si armonizzano con il comunitarismo e i clan della cultura giapponese, è però indicativo che, solo dopo pochi mesi di distanza dall'entrata in vigore della legge del 2005, si sia cominciato a dibattere in Giappone su come modificare molte sue disposizioni, affidando magari alle organizzazioni e alle compagnie per le quali lavorano i soggetti di cui si vogliono tutelare i "dati personali", la protezione degli stessi (Orito e Murata 2007: 448).

Per offrire un altro esempio, questa volta più vicino all'esperienza e sensibilità del lettore italiano, si pensi al codice di procedura penale, detto anche codice Vassalli, introdotto con decreto del presidente della repubblica il 22 settembre 1988, n. 447, ma in realtà in vigore a partire dall'ottobre 1989. A grandi linee, rispetto al precedente codice Rocco, imperniato sul modello inquisitorio, il "nuovo" codice s'ispirava al principio di parità delle parti, tra pubblica accusa e difesa, proprio del modello accusatorio tipico dei sistemi di common law, prevedendo inoltre meccanismi di economia processuale, spesso con taglio spiccatamente pragmatico, come nel caso del patteggiamento. Innestato in una cultura giuridica affatto diversa e con principi costituzionali per molti versi antitetici al nuovo sistema processuale – come, ad esempio, nel caso della "verità processuale" che male si concilia con molti profili pragmatici del sistema accusatorio – ben presto anche in Italia, e sia pure per motivi diversi da quelli prima accennati in Giappone, si è assistito a un'analoga crisi di rigetto.

Per illustrare il punto, conviene tornare ad alcuni elementi di teoria delle reti di cui siamo già esperti (§ 2.2.2.1). All'inizio del 2014, con i colleghi dell'istituto di

teoria e tecniche dell'informazione giuridica di Firenze (ITTIG), abbiamo cominciato a ordinare l'insieme di tutte le pronunce emesse in via incidentale dalla Corte costituzionale italiana a far data dal 1956, al fine di capire come la corte citasse i propri precedenti, con quali leggi di distribuzione e se, al modo di altri tribunali, come la Corte di giustizia di Lussemburgo o la Corte suprema di Washington, anche la casistica della Consulta di Roma s'imperniasse su pochi grandi hub. A partire dal febbraio 2014, grazie al lavoro di Tommaso Agnoloni e sotto la direzione di Daniela Tiscornia, abbiamo cominciato così a scoprire, o ad avere conferma, che anche per il reticolo giurisprudenziale della Consulta valgono le leggi di potenza illustrate nel capitolo secondo!

I primi risultati (straordinari) della ricerca possono essere illustrati con la prima figura del presente capitolo, in cui l'asse delle ascisse sul piano cartesiano quantifica il valore dei casi, mentre quello delle ordinate il loro ammontare nei gradi di distribuzione della rete. Come chiarisce a continuazione la figura 29, si ha a che fare ancora una volta con una "lunga coda" in cui pochi casi fungono da ponte d'informazione per la gran massa delle sentenze – si tratta per la precisione di 15020 giudizi in via incidentale – che compongono il sistema in esame:

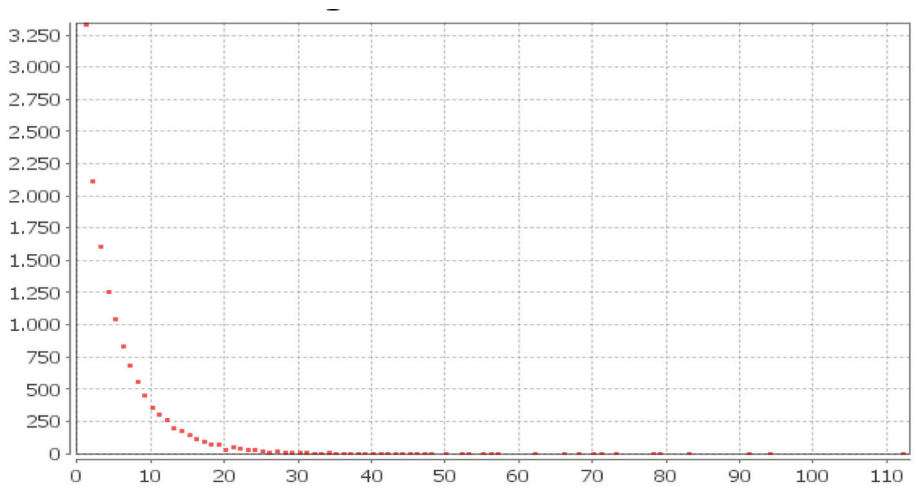


Figura 29: *La lunga coda della Consulta*

Pur non insistendo sul merito di una ricerca ancora in corso, basti qui dire che un considerevole numero di hub del reticolo, ossia le sentenze che più spesso la Corte di Roma cita tra i propri precedenti, sta a illustrare, non a caso, ciò che abbiamo designato come la crisi di rigetto che è oggetto del presente paragrafo. Dei 25 casi maggiormente ripresi dalla Consulta lungo la sua lunga coda, ben sei riguardano il diritto penale: è proprio il caso di dire che la lingua batte dove il dente del paese duole!

In particolare, dei casi che ci riguardano [1], si deve annoverare all'11° posto la sentenza 313 del 1990 sui procedimenti speciali e l'applicazione della pena su richiesta delle parti, con i poteri affidati ai giudici e il possibile contrasto con il principio di soggezione soltanto alla legge. Al 24° posto, troviamo la sentenza 89 del 1996 sulle misure cautelari personali, in specie la custodia in carcere, e il termine massimo di quella misura nel caso di procedimenti per più reati in rapporto di connessione qualificata. Se poi restringiamo l'indagine all'arco temporale che va dal 1989 a metà 2014, la predetta sentenza 313/1990 sale dall'11° al 6° posto, la 89/1996 all'8°, cui va ad aggiungersi, al 17°, la sentenza 432 del 1995 in tema di dibattimento e l'incompatibilità per il giudice che nel corso delle indagini preliminari abbia disposto una misura cautelare personale nei confronti del rinviato a giudizio; e al 22° la sentenza 131 del 1996, ancora in tema di dibattimento, ma a proposito del giudice che, quale componente del tribunale della libertà o in appello, abbia concorso a pronunciare un provvedimento sulla libertà personale.

Ma, senza dover proseguire oltre con i dettagli della ricerca, il suo ammonimento a questo punto dovrebbe essere chiaro. Anche nel caso dei trapianti giuridici valgono i criteri normativi messi a punto fin dal terzo capitolo, circa "il dovere di conoscenza" (§ 3.4.3.2), e "la scelta degli strumenti" (§ 3.4.3.3), da parte dei legislatori.

Il prezzo per disattendere simili criteri, è dato infatti dalle crisi di rigetto.

### 10.2.2. *Operazioni di successo*

Un segno benaugurante per chi abbia intenzione di prendere a prestito istituzioni, concetti o strutture, con la formula di Alan Watson, è dato dai casi nei quali l'operazione di trapianto giuridico ha avuto esito positivo. Tra gli innumerevoli esempi possibili basti qui riportarne due; uno per ciascuna delle parti, generale e speciale, del presente libro.

Da un lato, il richiamo si volge alla costituzione dei moderni (§ 3.1.3.1), ossia all'insieme mirabile delle idee con cui i padri fondatori americani diedero forma a una repubblica fondata sui principi della sovranità popolare, riconoscimento dei diritti naturali, divisione dei poteri, rigidità del costrutto e tutela giurisdizionale costituzionale, entro il quadro definito dalla struttura federata dell'Unione. Sebbene, come s'è detto, più che di un passaggio o snodo, il trapianto è avvenuto in molti paesi a séguito di moti rivoluzionari o degli effetti catastrofici di una guerra, chiaro è che la circostanza di per sé non garantisce o spiega il successo dell'operazione di trapianto; e, comunque, essa sta a confermare la tesi di Watson, che cioè i trapianti giuridici vadano annoverati tra le fonti principali dell'evoluzione del fenomeno giuridico.

D'altro canto, si pensi al caso della tutela dei dati personali in Italia (v. § 4.3.1). Allorché il Parlamento di Roma ha approvato la legge 675, s'innestava per la prima volta nell'ordinamento italiano un consistente gruppo di norme in materia di raccol-

[1] Oltre al campo processual-penalistico vigente oggi in Italia e di cui ci occupiamo nel testo, il lettore attento e curioso può ben domandarsi che ne è delle altre sentenze della Consulta esaminate in questo libro. Mi limito a segnalare la fondamentale pronuncia del caso *Granital* (§ 3.2.2): essa appare al 30° posto della classifica generale.

ta, trattamento e uso dei dati personali, a cui si era stati in certo qual modo costretti, dato che il recepimento della direttiva 46 del 1995 rappresentava la condizione indispensabile per godere dei benefici legati agli accordi sottoscritti a Schengen il 14 giugno 1985 e, poi, inclusi nell'omologa Convenzione del 19 giugno 1990. La grande novità rappresentata dal poter viaggiare liberamente attraverso l'Unione, senza più dover mostrare il proprio passaporto, era infatti subordinata allo standard comune di tutela nella libera circolazione dei dati. Il fatto, poi, che il Parlamento italiano abbia approvato la 675 il martedì 31 dicembre 1996 verso sera, non è certo dipeso dalla solerzia, o stakanovismo, dei nostri politici, decisi a passare la nuova legge entro l'alba del nuovo anno. Piuttosto, più prosaicamente, la circostanza è dipesa dal fatto che quello era l'ultimo giorno entro il quale gli stati membri dell'Unione avrebbero dovuto recepire la normativa comunitaria (nel caso in cui, beninteso, essi avessero voluto far parte degli accordi di Schengen).

Nonostante il pressapochismo iniziale, qualche incidente di percorso (§ 6.2.4, a proposito dei redditi degli italiani online), o i problemi tuttora aperti (§ 9.2), si può dire che a quasi vent'anni di distanza da quella prima legge, il giudizio da dare su questa forma di trapianto giuridico sia in sostanza più che positivo. Si è formata in Italia una cultura della privacy informazionale che prima, semplicemente, non esisteva, grazie anche al solerte lavoro di chi, dal 1997 al 2005, è stato il primo presidente del Garante italiano per la protezione dei dati personali, Stefano Rodotà (v. § 5.5).

Alla luce di queste operazioni di successo, per seguire con le metafore mediche, si tratta pertanto di provvedere a esportare ora il test di Harlan in Europa. Riprendendo i criteri normativi elaborati nel capitolo terzo, occorre spiegare innanzitutto perché ciò sia necessario (§ 3.4.3.1); quanto richiede, a sua volta, un dovere di conoscenza (§ 3.4.3.2), al fine di precisare gli strumenti giuridici da trapiantare (§ 3.4.3.3).

## 10.3. *L'esportazione del test*

Si è fatto cenno al fatto che i trapianti giuridici non solo interessano istituzioni o strutture, ma anche concetti. La distinzione proposta da Alan Watson è particolarmente rilevante in questo contesto, stante le differenze tra Stati Uniti ed Europa circa il modo in cui può essere colta l'idea di cui si fa carico il test di *justice* Harlan. Mentre, nel paese d'origine, la "ragionevole aspettativa di privacy" funge da parametro di costituzionalità per la sfera del gubernaculum sotto l'egida del quarto emendamento, invece, in Europa, questa medesima aspettativa è piuttosto plasmata dal legislatore. Come abbiamo visto nel precedente paragrafo a proposito dell'Italia, è stato in fondo il legislatore di Roma, sia pure costretto dagli impegni comunitari, a dare il via a una cultura della privacy informazionale proprio a partire dalla legge 675 del 1996.

Il fatto, però, che questa cultura si sia formata e che, anzi, essa vanti in altri paesi europei ormai quasi quarant'anni d'esperienza, come in Svezia o in Germania (§ 6.1.2), sta a suggerire che anche tra i cittadini del vecchio continente si è venuta formando qualcosa di simile alla pretesa che i cittadini americani vantano nei confronti del proprio governo e nelle relazioni tra privati; ossia, una ragionevole aspettativa di privacy. Sul piano normativo, infatti, gli individui si attendono e, dunque, preten-

dono al di qua dell'Atlantico, che i propri dati siano usati per i fini per cui è stato chiesto loro il consenso, e che quei dati non siano ceduti o concessi a terzi, o che se ne possa avere l'accesso per ottenere, se del caso, la rettifica. Questa pretesa normativa europea non cancella ovviamente le differenze, che pur persistono al di qua e al di là dell'Atlantico, quanto al contenuto della pretesa o riguardo ai meccanismi istituzionali con cui essa può farsi valere. Abbiamo del resto segnalato come non esista, allo stato, qualcosa di simile al Quarto emendamento in Europa (§ 8.1); e che, anche nel vecchio continente, rimangono notevoli differenze, per cui, ad esempio, sarebbe difficile immaginare in Italia, le proteste che si sono avute invece in Germania per via dei servizi di mappe e strade di Google (§ 6.2.4).

Tali differenze di forma e di sostanza evidenziano come non si tratti d'esportare in Europa istituzioni e strutture americane sulla ragionevole aspettativa di privacy. Come già nel caso dell'originario impianto accusatorio del codice di procedura penale in Italia, assisteremmo, nella migliore delle ipotesi, a una crisi di rigetto. Le differenze di cultura e sensibilità giuridica stanno a indicare piuttosto come si tratti di trapiantarne un concetto e, soprattutto, i limiti secondo cui cogliere l'applicabilità del concetto stesso in Europa.

A ben vedere, il test non può infatti svolgere nel vecchio continente lo stesso ruolo che esso ha nel paese d'origine – vale a dire, fungere da parametro di legittimità costituzionale delle azioni del gubernaculum – in ragione del fatto, innanzi accennato, che sono proprio i principi della direttiva 46 del '95 a rappresentare il parametro della ragionevole aspettativa di privacy in Europa. È su queste basi che sono state poi predisposte le disposizioni di rango costituzionale introdotte con la Carta UE dei diritti fondamentali (2000), recepite formalmente solo con il successivo trattato di Lisbona del 2009 (v. § 6.3.3). Per cui, se dal punto di vista astrattamente formale e della gerarchia delle fonti, sono queste ultime disposizioni a essere sovraordinate alla direttiva 46, all'atto pratico è stata questa normativa a introdurre le garanzie costituzionali sulla privacy informazionale in Europa. Pragmaticamente, non avrebbe senso esportare il test di Harlan nel vecchio continente, semplicemente per valutare la bontà dei principi della prima direttiva comunitaria che, a loro volta, fondano i presupposti per svolgere il test medesimo. Quale, dunque, le ragioni per tentarne nondimeno il trapianto?

A continuazione, ne propongo in definitiva tre: la prima riguarda la differenza tra la prima direttiva comunitaria del '95 e la successiva legislazione derivata (§ 10.3.1).

Dopo di che, l'attenzione sarà ancora una volta incentrata sulle sfide e i problemi che la rivoluzione tecnologica è pronta a proporre (§ 10.3.2).

Infine, il rimando andrà a un curioso vuoto dottrinale (§ 10.3.3).

Su queste basi, trattandosi d'esportare un concetto, piuttosto che un'istituzione o struttura giuridica, saremo pronti a esaminare l'intera ragionevolezza dell'operazione.

### 10.3.1. *Critica del giudizio*

L'assonanza kantiana del titolo di questo paragrafo non è affatto casuale. Dopo i rimandi alla definizione che Kant offre del diritto (§ 1.1.3), al progetto cosmopolitico messo a punto nel saggio *Per la pace perpetua* (§§ 3.3.2, 4.2.2 e 4.3.2), e con la

fondazione del diritto pubblico in chiave anti-paternalistica nel *Contro Hobbes* (§ 5.3.3.1), il richiamo alla terza critica di Kant, la *Critica del giudizio* (1790), serve qui a introdurre il primo ordine di considerazioni per le quali, a mio avviso, il test di Harlan può essere convenientemente trapiantato e impiegato in Europa. Rimandando a breve gli spunti da trarre dalla terza critica kantiana, occorre innanzitutto prendere in esame i giudizi che i giudici danno nel dirimere le controversie dell'ordinamento, secondo la ridondanza dei termini su cui abbiamo già avuto modo d'insistere nel capitolo quarto (§ 4.1.2).

In sostanza, ci si è soffermati in precedenza sulla tesi che il test non possa fungere in Europa da metro di valutazione critica dei principi della direttiva 46 del 1995, per la semplice ragione che, proprio sulla base dei principi di questa normativa, si è venuta formando una ragionevole aspettativa di privacy informazionale nel vecchio continente. Ciò non significa, va da sé, che talune norme o applicazioni della direttiva non possano essere sottoposte a critica; anzi, fin dalla sua presentazione nel capitolo ottavo (§ 8.1.3), si è posto l'accento su alcuni eccessi di zelo o di tutela, illustrati con l'esempio dei dati sensibili o con la difficoltà di riusare i dati personali raccolti e trattati nel settore pubblico (§ 8.4). Nondimeno, un conto è la critica, più che legittima, di talune disposizioni del diritto comunitario; altra cosa, però, è condurre questa valutazione critica in ragione di un test che si mira a proporre come banco di prova per quelle stesse disposizioni. Essendo i principi di queste ultime disposizioni alla base della aspettativa di privacy in Europa, il risultato sarebbe un "non sequitur", una conclusione illogica.

Analoghe considerazioni sembrano del resto valere anche per la successiva legislazione europea, come nel caso, già menzionato (§ 8.4.4.1), della direttiva 24 del 2006 sulla ritenzione dei dati, oppure, a proposito degli obblighi dei fornitori di servizi in rete nei confronti del sedicente diritto all'oblio, secondo la formula impiegata anche dalla Cassazione italiana (§ 9.2.3). Si tratta dei casi in cui la Corte di Lussemburgo è stata chiamata a esprimere il suo giudizio di legittimità costituzionale sulla legislazione derivata, in ragione dell'interpretazione e applicazione dei principi e norme contenute nella Carta UE dei diritti fondamentali e nei trattati dell'Unione. Più che sul test della ragionevole aspettativa di privacy informazionale, pertanto, la questione pare vertere esclusivamente sul modo in cui quei principi e norme di rango costituzionale sono intesi dalla Corte; come, del resto, essa ha fatto l'8 aprile 2014, nel rifarsi soprattutto agli articoli 7 (privacy tradizionale) e 8 (protezione dati) della Carta, per dichiarare l'invalidità dell'intera normativa di cui alla D-2006/24/CE.

Rispetto a D-95/46/CE, tuttavia, esiste una differenza di fondo, che lascia spazio all'esportabilità e ruolo specifico che può svolgere in questo caso il test. Stante, infatti, la generalità e astrattezza dei principi che la Corte di giustizia è chiamata a far valere, sia pure temperati dalla concretezza dei richiami ai propri precedenti giurisprudenziali, c'è modo di testare la bontà delle decisioni prese nei termini della ragionevole aspettativa di privacy, nel senso che quanto è ragionevole attendersi e, dunque, pretendere dall'autorità costituita, può servire da criterio di valutazione della stessa ragionevolezza e legittimità delle decisioni prese sia dal legislatore sia, eventualmente, da parte dei giudici. In fondo, è stato questo l'assunto su cui hanno insistito alcuni cittadini e organizzazioni, nelle cause intentate in Irlanda e Austria contro le normative nazionali che avevano provveduto al recepimento della direttiva

24 sulla ritenzione dei dati; e che, poi, con il consueto meccanismo del rinvio pregiudiziale alla corte, sarebbero approdate in Lussemburgo per sincerarsi della legittimità comunitaria di quella direttiva. Per esprimere le lamentele degli attori con le parole della Corte, "la Direttiva 2006/24 tocca, in maniera generalizzata, tutte le persone che usano servizi di comunicazione elettronica, ma senza che quelle persone, i cui dati vengono conservati, si trovino, anche indirettamente, in una situazione che possa dar luogo a un procedimento penale. La direttiva pertanto si applica anche a persone per le quali non c'è alcun tipo di evidenza che possa suggerire che la loro condotta sia riconducibile, anche indirettamente o in forma remota, a un crimine grave" (C-293/12, § 58). Inoltre, prosegue la Corte, "nel cercare di contribuire alla lotta contro gravi crimini, la Direttiva 2006/24 non prevede nessuna connessione tra i dati per i quali si chiede la conservazione, e una minaccia alla sicurezza pubblica e, in particolare, la direttiva non prevede limiti alla ritenzione dei dati né in rapporto (i) a dati concernenti un particolare arco di tempo e/o una particolare area geografica e/o la cerchia di un particolare gruppo di persone che è probabile siano coinvolte, in un modo o nell'altro, in un crimine grave, né in rapporto (ii) a persone che potrebbero, per altri motivi, contribuire, per via della ritenzione dei loro dati, a prevenire, rilevare o perseguire crimini gravi" (*op. cit.*, § 59).

Questo irragionevole scenario cui ha dato luogo la direttiva 24, come riferito (§ 8.4.4.1), è stato dichiarato dalla Corte illegittimo e, dunque, invalido, perché in contrasto con il principio di proporzionalità.

Tuttavia, anticipando alcuni degli spunti da trarre dalla *Critica del giudizio* di Kant, ben possono rovesciarsi i termini della questione e, di qui, asserire sul piano filosofico che la direttiva 24 non è apparsa irragionevole perché sproporzionata ma, al contrario, sproporzionata perché irragionevole. Anche il più incallito formalista tra i cultori del diritto europeo, in fondo, dovrebbe ammettere che è il principio di proporzionalità a dipendere dall'idea di ragione e non, viceversa, che la ragione debba essere di per sé proporzionata. A conferma, basterebbe ricordare come nel capitolo quinto (§ 5.4.3), ci siamo già occupati di un altro caso deciso dalla Corte di giustizia in cui, sempre riguardo alla tutela della privacy, la corte si è pronunciata per l'incompatibilità delle pretese attoree con il quadro della legalità comunitaria, con il risultato che nessuna opera di bilanciamento, o proporzionalità, tra le misure richieste e i danni lamentati, è stata necessaria in quella circostanza. Oltre a opere di bilanciamento e proporzionalità, in altri termini, esistono anche decisioni che ragionevolmente prevedono una logica "a somma zero".

Inoltre, nello spostare in questo modo il fuoco dell'attenzione sul piano della ragionevolezza del giudizio, si consegue un ulteriore risultato. A differenza di altre corti, come quella Suprema americana o il Tribunale costituzionale tedesco, la Corte di Lussemburgo non rende note (purtroppo) le proprie opinioni concorrenti o dissenzienti. Di qui, mancando il riferimento all'autorità, sia pure minoritaria, di un membro della corte, il punto da cui muovere per ogni riflessione critica, non può che fare affidamento al punto di vista della ragione. È quest'ultima la fonte comune per vagliare sia la bontà delle aspettative di tutela dei consociati, sia la sostanza delle stesse sentenze della Corte. Basti in fondo ripensare al caso *Costeja González vs. Google* (§ 8.5.2.2), dove si è sottolineata l'irragionevolezza della lettura offerta dalla corte su alcuni articoli chiave della direttiva 46, che hanno consigliato di rifarsi al

principio ermeneutico di carità di Davidson per limitare almeno i danni. In tutti questi casi in cui occorre valutare i giudizi dei giudici, si tratta in definitiva di quella nozione di "ragionevolezza informativa" introdotta nel capitolo precedente (§ 9.3.3), che avremo occasione di riprendere e approfondire ulteriormente nei paragrafi che seguono. Per ora, basti dire con la *Critica del giudizio* di Kant, che "la necessità dell'accordo universale, che è pensata in un giudizio […] è una necessità soggettiva, che è rappresentata come oggettiva con la presupposizione di un senso comune" (*op. cit.*, § 22). È proprio questa idea di un senso che abbiamo in comune con gli altri che rinvia, secondo Kant, a "una facoltà di giudicare che nella sua riflessione tiene conto *a priori*, del modo di rappresentare di tutti gli altri, per raffrontare in qualche forma il proprio giudizio nei limiti della complessiva ragione umana" (*op. cit.*, § 40).

### 10.3.2. *Prolegomeni a ogni legislazione futura*

Il secondo scenario nel quale l'esportazione del test di Harlan risulta fruttuosa e opportuna, non riguarda più il giudizio sulla ragionevolezza relativa all'applicazione della legislazione vigente, quanto alla progettazione di ogni legislazione futura; vale a dire su ciò che è lecito che i cittadini europei si attendano, e pretendano, nel caso in cui i propri legislatori mirino a intervenire nel settore di tutela della privacy informazionale. Il richiamo appunta sia agli aspetti problematici della proposta di regolamento presentata dalla Commissione e, poi, largamente emendata dal Parlamento europeo, sia ai paragrafi conclusivi del capitolo precedente in cui, esaminando le sfide che la rivoluzione tecnologica è pronta a proporre con una nuova generazione di droni, con la robotica di servizio e gli ambienti intelligenti, è sorto il problema di prendere posizione su quale possa essere la ragionevole aspettativa di privacy in queste situazioni. Alla necessità d'integrare con il parametro normativo della ragionevolezza l'interpretazione dei testi di legge nella risoluzione dei casi, va così ad aggiungersi l'utilità di questo criterio, quando siano le istituzioni stesse a essere divise, come è avvenuto con la Commissione e il Parlamento sul nuovo regolamento; oppure, quando i testi discussi da legislatori e autorità rimangano silenti sui problemi imminenti che la "quarta rivoluzione" sta per innescare.

A conferma dell'assunto circa l'utilità del test, è sufficiente soffermarsi sul tenore del comunicato stampa rilasciato dalla Commissione europea il 12 marzo 2014, riportato in nota nel capitolo sesto (v. § 6.2.4), allorché, con 621 voti a favore, 10 contrari e 22 astenuti, "il Parlamento europeo ha oggi cementato il forte appoggio, previamente dato a livello di comitato, alla riforma sulla protezione dei dati della Commissione europea". Con le parole della commissaria europea alla giustizia, Viviane Reding, "il messaggio che il Parlamento europeo sta mandando è inequivocabile: questa riforma è una necessità, e ora è anche irreversibile. I parlamentari direttamente eletti dall'Europa hanno dato ascolto ai cittadini e uomini d'affari europei e, con questo voto, hanno reso chiaro che abbiamo bisogno di un'uniforme e robusta normativa per la protezione dei dati, che renderà la vita più semplice per gli affari e rafforzerà la protezione dei nostri cittadini".

Tra gli antefatti del processo di riforma legislativa, su cui siamo venuti insistendo nel corso dei capitoli precedenti, è particolarmente significativo che il comunicato

stampa della Commissione sottolinei la "chiara necessità di porre rimedio alla crescente frattura tra gli individui e le compagnie che trattano i loro dati", riportando alcuni dati statistici del rapporto sulle "attitudini sulla protezione dati e l'identità elettronica nell'Unione europea", a cura dell'Eurobarometro 359 del giugno 2011[2]. Scopriamo così, tra le altre cose, che il 92% degli europei dicono di essere preoccupati sulle applicazioni dei propri cellulari che raccolgono i dati senza il relativo consenso e che circa il 70% è del pari assillato dall'idea che le compagnie e società con cui intrattengono rapporti, possano trasmettere quelle informazioni a terzi. Ne emerge un quadro ricco e compatto, per molti versi affascinante, di quale sia oggi la ragionevole aspettativa di privacy in Europa che, a torto o a ragione, la Commissione e il Parlamento avrebbero preso in considerazione, al momento di varare la riforma della direttiva 46 del '95.

Nell'apprezzare quantomeno lo sforzo delle istituzioni europee di rimanere in sintonia con l'evolversi delle dinamiche sociali nel vecchio continente, tuttavia, al pari di quanto precedentemente rilevato a proposito del test sulla ragionevole aspettativa di privacy in America (§ 7.5), occorre prevenire un possibile malinteso. Il fatto, cioè, che i cittadini europei abbiano le idee piuttosto chiare su ciò che essi si aspettano sia loro tutelato della propria privacy informazionale, non significa rendere l'intervento del legislatore superfluo, tanto più in un'epoca di vertiginosa innovazione tecnologica in cui, come già detto, quella stessa aspettativa di privacy non può che essere "in flusso". Ma ammettere, con le parole di *justice* Alito nel caso Jones (§ 7.4.1.1), che "un corpo legislativo è bene collocato per misurare il mutamento delle attitudini sociali, per definire linee ben precise e bilanciare la privacy con la sicurezza pubblica in un modo comprensibile", non comporta affatto ricadere nella posizione formalistica di chi vede nella legislazione una sorta di parametro autoreferenziale con cui determinare ciò che è ragionevole, o meno, attendersi sia protetto dall'ordinamento. Alcune delle disposizioni alquanto discutibili che, tra Parlamento e Commissione, sono venute delineandosi negli ultimi anni per via della riforma della direttiva 46, stanno piuttosto a ricordare l'ulteriore funzione che il test sulla ragionevole aspettativa ha in questi casi. Come anticipato nel paragrafo precedente, occorre infatti mettere ancora alla prova la ragionevolezza di ogni legislazione futura, per cogliere il paradosso di un silenzio dottrinale. È qui che torna nuovamente utile il richiamo alla *Critica del giudizio* di Kant.

### 10.3.3. *Un paradosso dottrinale*

Dobbiamo a una filosofa a noi nota, Hannah Arendt (v. § 6), il recupero in chiave politica di un'opera come la terza critica di Kant, che sembra rivestire poca o nessuna rilevanza per la riflessione del giurista. Come noto, la critica del giudizio di Kant si configura innanzitutto, sul piano estetico, come giudizio del gusto che, per il filosofo tedesco, appare essenzialmente libero e scevro da ogni tipo di interesse, svincolato dalla logica della necessità e dalla cogenza, categorica o ipotetica, dell'imperativo. Nella sua dimensione propria, resa banale dall'adagio popolare attorno a

[2] Si v. *http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf*.

ciò che è bello, si può pertanto dire che il gusto è sempre teso a cogliere l'individualità concreta e singola, e mai concetti astratti.

Tuttavia, se anche dal giudizio di gusto, nella sua accezione kantiana, scaturisce "l'impossibilità di derivare un qualsiasi prodotto particolare della natura da cause generali", è pur sempre Kant a sottolineare il carattere condizionato, necessitato e dialogico di questo giudizio. Da un lato, si legge nel § 19 della terza critica, la "necessità soggettiva, che attribuiamo al giudizio di gusto, è condizionata", nel senso che "il giudizio di gusto esige il consenso di tutti; e chi dichiara bella una cosa pretende che ognuno dia l'approvazione all'oggetto in questione, e debba dichiararlo bello allo stesso modo". D'altro canto, aggiunge Kant nel § 20, "la condizione di necessità, che presenta un giudizio di gusto, è l'idea di un senso comune" che – come riferito poco fa – comporta di tener conto, nel giudicare, "del modo di rappresentare di tutti gli altri, per raffrontare in qualche modo il proprio giudizio nei limiti della complessiva ragione umana" (si v. ancora sopra § 10.3.1).

Questa natura condizionata, necessitata e dialogica dell'estetica kantiana la si ritrova del pari nel giudizio giuridico come problema di consenso, senso comune e limiti della ragione umana, specialmente allorché, come in questi paragrafi, ci si pone il problema di giudicare norme e decisioni sulla tutela della privacy informazionale, sulla base di un test relativo alla ragionevole aspettativa di tutela degli individui. Fin dai primi capitoli di questo libro, in fondo, siamo venuti osservando come le norme del diritto non operino in una sorta di vuoto pneumatico, ma abbiano a che fare piuttosto con le pratiche sociali di una data comunità, per cui il luogo normativo dell'autorità politica, più che dalla legge, è rappresentato dalla convenzione supportata dalla legge, ossia dalla convenzione tesa a risolvere il problema del coordinamento morale, che trasmette la sua autorità normativa alla struttura sociale oggetto dell'analisi (v. infatti §§ 1.1.1, 3.1.1 e 4.3.1). Di qui, uno dei meriti che abbiamo riconosciuto al test elaborato dalla Corte suprema negli ultimi cinquant'anni, è stato di fungere da ponte tra le norme e aspettative della società e le leggi e decisioni prese dall'ordinamento, secondo quel circolo virtuoso tra individuo, società e sistema giuridico che, messo a punto negli Stati Uniti d'America, abbiamo inteso trapiantare come banco di prova per valutare il modello europeo.

Riepilogando in termini kantiani la questione, si può dire che, innanzitutto, siamo partiti dai casi in cui la legislazione vigente in Europa è entrata in contrasto con le aspettative di privacy degli individui che, per ciò stesso, sono stati pronti a difendere le proprie ragioni in tribunale: dalla ragionevole aspettativa di privacy siamo passati perciò alla necessità kantiana di giudicare i giudizi dei giudici nei limiti della complessiva ragione umana.

Dopo di che, il test si è esteso a ogni legislazione futura e a ciò che gli individui possono ragionevolmente pretendere venga loro protetto in funzione delle proprie aspettative, con gli ulteriori principi kantiani del condizionamento del consenso e la necessità di un senso comune.

A completamento di quanto detto, bisogna però ora aggiungere un paradosso e, cioè, come la ragionevole aspettativa di privacy, che pur esiste tra i cittadini europei, finisca nondimeno per non trovare spazio alcuno nella dottrina giuridica del vecchio continente; e, questo, nonostante il carattere kantianamente dialogico, condizionato e necessitato del giudizio.

In ultima analisi, le ragioni del silenzio possono essere di tre tipi: il primo riguarda implicitamente il giudizio sull'inesportabilità del costrutto, vuoi nel caso particolare, vuoi in generale, come opzione ideologica di fondo. Come tuttavia è stato opportunamente notato (Graziadei 2009), "lo studio dei trapianti giuridici […] conduce a riflettere sulle questioni di giustizia che trascendono i confini di un singolo sistema giuridico, confrontandole con le sfide della diversità tra comunità e individui". Su tali questioni di giustizia torneremo a breve nel prossimo paragrafo.

In secondo luogo, il silenzio può dipendere dal fatto che si esaminano gli stessi problemi ma con linguaggio più consueto al giurista europeo, per cui, piuttosto di una ragionevole aspettativa di privacy informazionale, si discorre in termini di proporzionalità o di tutela dei diritti fondamentali o di bilanciamento. Per i motivi detti, in sede filosofica sembra nondimeno pacifica la necessità di ricondurre questi criteri ermeneutici alla ragione, piuttosto che procedere all'incontrario, ricavando la medesima induttivamente dai singoli casi di tutela. Altrimenti, come prendere posizione tra una decisione bilanciata e una che, viceversa, opta per un giudizio "a somma zero"?

Infine, il silenzio può essere consigliato dalla necessità di non ricadere in opzioni di tipo giusnaturalistico, contrapponendo ai principi dell'ordinamento, o alla legislazione vigente, o alle decisioni dell'autorità costituita, i parametri di una razionalità incerta o non ben definita. Anche in questo caso, però, la preoccupazione è infondata se, come riferito (§ 9.3.2), la tesi della "ragionevolezza informativa" ha preso le mosse da un campione della scuola analitica come Herbert Hart e dalla critica alle tesi di chi, come Ronald Dworkin, ha inteso ottenere un'unica "risposta corretta" per ogni caso difficile del diritto, in ragione di una teoria moralmente coerente.

Nel riprendere le considerazioni svolte in quella sede, si ricorderà infatti come, anche a presentare il diritto sotto la sua migliore veste, sia stato indispensabile affrontarne alcuni casi con un certo margine di tolleranza, per venire incontro sia ai fenomeni d'incompletezza che valgono per il linguaggio che ha di mira il mondo del diritto, sia ai suoi casi difficili, avendo a mente le distanze che corrono tra i sistemi giuridici, o le disparità di vedute all'interno di un ordinamento dato.

A continuazione, occorre approfondire queste considerazioni sul piano normativo dell'informazione per la realtà, inoltrandoci nei terreni degli ideali di giustizia maturati in sede morale e dei suoi rapporti con lo spirito di tolleranza. Il proposito è di mettere in chiaro le diverse accezioni secondo cui la nozione di tolleranza del test può essere qui intesa, in rapporto alle questioni di giustizia che le operazioni giuridiche di trapianto finiscono per sollevare. Su queste basi, potremo concludere il capitolo con la prova del test.

## 10.4. *La tolleranza del test*

Dopo aver circoscritta l'indagine sul piano della privacy informazionale (§ 10.1), e chiarita del pari la nozione di trapianto giuridico (§ 10.2), si è specificato il senso in cui il test della Corte suprema americana sia utile anche nel caso del modello europeo (§ 10.3). Il prossimo passo consiste nel precisare ulteriormente il livello di astrazione dell'analisi, a proposito della ragionevolezza informativa che il test propone in nome della tolleranza.

Innanzitutto, si può fare riferimento alla nozione di ragione, veicolata dal test, in accordo con lo spirito di chi rispetta le altrui opinioni e non ne ostacola la libera estrinsecazione, nonostante le disparità di vedute che possano sussistere in merito. Si tratta di una definizione sufficientemente ampia di tolleranza, riconducibile in parte a chi abbiamo già indicato come uno dei precursori delle dichiarazioni dei diritti dell'uomo e padre del liberalismo moderno, John Locke (§ 3.3.1). Questo è l'approccio che, in fondo, ha ispirato la presente ricerca sulle differenze che in materia di privacy esistono tra il modello americano e quello europeo, nonché a proposito delle modalità secondo cui è possibile trapiantare nel vecchio continente un test maturato in una cultura e tradizione giuridica affatto diverse.

Tuttavia, bisogna ora sottolineare come questa posizione non sia affatto pacifica, tanto per una ragione filosofica generale, come per una specifica in tema di privacy. Sul primo fronte, si rinvia a un'idea prevalsa alla fine tra i moderni e che trova per molti versi un punto di orientamento indiscusso nella filosofia pratica di Kant. Il concetto di tolleranza andrebbe infatti ricondotto al principio di giustizia, e non viceversa, dato che si può ben pensare a un eccesso di tolleranza, ma mai a un eccesso di giustizia. Si tratta di una tesi che, come diremo, ha trovato nello scorso secolo illustri sostenitori, tra cui un filosofo che conosciamo, Karl Popper (v. § 8.4.1).

D'altro canto, sul piano specifico della privacy informazionale, il paradosso della tolleranza può essere illustrato con le tesi dell'"effetto Bruxelles", esposte nel capitolo precedente (§ 9.1). In quella sede si notava come, a differenza di altri settori, come per esempio il mercato del lavoro, risulterebbe difficile concepire all'interno di un unico ordinamento, una molteplicità di discipline giuridiche che convivano in tema di privacy. Infatti, le difficoltà che le imprese hanno d'isolare, nelle proprie banche dati, le informazioni di cui esse hanno bisogno per svolgere un'attività mirata a un solo paese, spiega perché esse abbiano più spesso finito per allineare le proprie attività globali agli standard del modello europeo.

Di qui un primo interrogativo: in che senso declinare in questa sede la tolleranza del nostro test? E ancora: come misurarsi con le questioni di giustizia che ogni trapianto giuridico propone? Quale il rapporto tra la ragionevolezza dell'intera operazione e la ragionevole aspettativa di privacy, su cui fa leva il test di Harlan?

Per affrontare questo nuovo insieme di questioni, conviene passare in rassegna quattro modi diversi in cui la nozione di tolleranza può essere intesa: ora riconducendola all'idea di giustizia (§ 10.4.1), ora concependo la tolleranza in forma autonoma (§ 10.4.2), ora come esito dell'insufficienza della giustizia quale parametro unico mediante il quale affrontare la complessità dei problemi in gioco (§ 10.4.3), ora come ragionevole indeterminatezza del test nell'affrontare i casi difficili del diritto (§ 10.4.4).

Chiarito in questo modo il senso specifico in cui la tolleranza del test è intesa, saremo finalmente pronti a metterlo alla prova, tornando al problema di quale possa essere la ragionevole aspettativa di privacy oggi in Europa (§ 10.5).

### 10.4.1. *Sui limiti della tolleranza*

Si è fatto cenno poco fa a come, nel primo volume de *La società aperta e i suoi nemici*, Karl Popper abbia insistito su ciò che chiamava il paradosso della tolleranza,

per cui una "tolleranza illimitata conduce necessariamente alla scomparsa della tolleranza. Se applichiamo una tolleranza illimitata anche a coloro che sono intolleranti, se non siamo preparati a difendere una società tollerante contro l'attacco violento dell'intollerante, allora il tollerante verrà distrutto e, con questo la tolleranza […] Dobbiamo pertanto sostenere, nel nome della tolleranza, il diritto di non tollerare l'intollerante. Dobbiamo ritenere che ogni movimento che rivendichi l'intolleranza si colloca al di fuori della legge, e dovremmo considerare l'istigazione all'intolleranza e l'oppressione come un'attività criminale, nello stesso modo in cui consideriamo l'istigazione all'omicidio, al sequestro, o il ritorno alla tratta degli schiavi, come criminale" (Popper ed. 2002).

Ad analoghe conclusioni, e sia pure sulla base di motivazioni diverse, sarebbe giunto quasi trent'anni dopo John Rawls (1921-2002), in quello che può essere considerato il più importante studio sulla teoria della giustizia negli ultimi cinquant'anni. Sebbene, a giudizio del filosofo statunitense, ogni società che aspiri a essere giusta debba essere tollerante – poiché, caso contrario, diventando intollerante, essa diverrebbe altresì ingiusta – andrebbe tuttavia riconosciuto, al pari di Popper, che ogni società abbia un ragionevole diritto alla propria auto-conservazione che prevale, in quanto tale, sullo stesso principio di tolleranza. Con le parole di Rawls, "se una setta intollerante non ha di per sé titolo a lamentarsi dell'intolleranza, la sua libertà andrebbe ristretta solo quando il tollerante crede sinceramente e a ragione che la propria sicurezza e quella delle istituzioni libere siano in pericolo" (Rawls 1971: 220).

Si tratta peraltro di un paradosso, quello della tolleranza, che non ha occupato soltanto i filosofi se, come riferito (§ 3.1.2), la costituzione democratica di Weimar finì a sua volta per consegnarsi tragicamente, e per via democratica, alla follia di Hitler. Questo aiuta a comprendere perché, nella successiva costituzione democratica di Bonn, sorta dalle ceneri del secondo conflitto mondiale, l'articolo 18 reciti che "chi abusa della libertà di espressione delle proprie opinioni, e in particolare della libertà di stampa (art. 5 comma 1), della libertà d'insegnamento (art. 5, comma 3), della libertà di riunione (art. 8), della libertà di associazione (art. 9), del segreto epistolare, telegrafico e telefonico (art. 10), del diritto di proprietà (art. 14) o del diritto d'asilo (art. 16, comma 2), per combattere i princìpi del libero ordinamento democratico, perde questi diritti fondamentali. La perdita e la misura della medesima sono pronunziate dalla Corte costituzionale federale".

La conclusione da trarsi da queste pur succinte considerazioni, è pertanto che per esercitare la tolleranza, occorra comunque averne stabilito dei limiti che, volta per volta, vanno individuati nella legge, la sicurezza o la libertà, oppure nell'abuso di queste libertà e diritti, come nel caso dell'odierna legge fondamentale tedesca. In ogni caso, i limiti che devono venire fissati per l'esercizio di una tolleranza equilibrata, non vanno individuati con la tolleranza stessa ma, piuttosto, in un ulteriore principio altro da sé che, come detto, più spesso, da Kant a Rawls, è stato identificato nel principio di giustizia. Si tratta in fondo dello stesso meccanismo in atto già con *La lettera sulla tolleranza* (1689) di Locke, dove il filosofo spiega le ragioni per le quali il principio avrebbe dovuto incontrare dei limiti sia riguardo agli atei sia ai cattolici.

Ma, lasciando da parte i crucci di Locke a proposito della religione (§ 3.1.1), occorre invece chiedersi dal punto di vista filosofico, stanno proprio così le cose?

### 10.4.2. *Sulla tolleranza dei limiti*

Dobbiamo a un filosofo cui abbiamo avuto modo di rifarci più volte nel corso di queste pagine, Luciano Floridi (§§ 1.4, 2.1 e 9.3.3), il più riuscito tentativo di venire a capo del paradosso della tolleranza[3]. Per stabilire i limiti del principio senza ricorrere a un criterio ulteriore, altro da sé, Floridi suggerisce di rappresentarne il concetto in rapporto a una relazione triadica, e non nei consueti termini diadici tra chi tollera e chi invece viene tollerato. Ne segue una conformazione formalmente analoga a quanto detto a proposito sia del contrattualismo politico moderno, a partire da Hobbes (§ 2.1.2.1), sia della teoria giuridica della giustizia con Locke (§ 3.1.1), entrambe imperniate su relazioni triadiche, ma con una differenza basilare.

Nel caso del contrattualismo moderno, il patto sociale tra le parti del contratto, chiamiamole "A" e "B", dà luogo all'istituzione di un terzo soggetto ("C"), il cui ruolo naturalmente cambia a seconda della variante del contrattualismo presa in esame: si avrà a che fare con un terzo superiore alle parti e svincolato dalle leggi, come nel contratto di Hobbes; un terzo vincolato, sia pure contraddittoriamente, alla tutela dei diritti naturali delle parti, come nel contratto di Locke; e così via, fino ai dilemmi sull'assenza del Terzo nel diritto internazionale, che abbiamo ripreso sulla scorta delle indicazioni di Bobbio (v. § 3.3.2).

Nel caso della teoria giuridica della giustizia, analogamente, il quadro prevede il rapporto tra quelle stesse parti, "A" e "B", le cui potenziali controversie vengono anche qui decise dall'intervento di un terzo soggetto ("C"), ora sopra le parti, come nel caso del diritto coattivo; ora tra le parti, come occorre invece nel diritto autoritativo. Riprendendo l'approccio evolutivo suggerito dal padre fondatore dell'economia politica moderna, Adam Smith (1723-1790), "il potere giudiziario sorge gradualmente dall'essere, in un primo momento, meramente una interposizione amichevole senza alcuna autorità legale che, nondimeno, avrà un effetto considerevole non appena questa terza persona abbia grande influenza su entrambe le parti" (Smith ed. 1978: 213). Ciò che qualifica in ogni caso l'intervento del terzo giudicante in chiave giuridica consiste nel fatto che esso sia equidistante dalle parti e disinteressato; ossia, scevro d'ogni conflitto di interessi.

Infine, tornando all'impostazione triadica della tolleranza proposta da Floridi, essa prevede tre soggetti posti su altrettanti piani diversi. Alla tradizionale versione diadica del principio tra chi tollera ("A") e chi è tollerato ("B"), deve infatti aggiungersi un terzo ("C"). Quest'ultimo è il destinatario delle azioni di chi viene tollerato ("B") da parte di "A" che, pur non condividendo le idee di "B", le rispetta, non impedendone l'estrinsecazione. Il paradosso evidenziato da Popper, Rawls, ecc., viene in questo modo superato, spostando il fuoco dell'attenzione sul terzo elemento "C" per appurare tre possibili casi:

i) che non ci sia affatto un "C", nel qual caso "A" potrà tollerare il fare o dire di "B" senza problemi particolari di sorta;

ii) che "C" esista ma non risenta significativamente dell'estrinsecazione di "B", nel qual caso vale per "A" la considerazione del punto precedente;

---

[3] Si tratta del saggio *Toleration and the Design of Norms*, in corso di pubblicazione su "Science and Engineering Ethics".

iii) che nel caso in cui "C" sia coinvolto in modo significativo dall'estrinsecazione di "B", "C" presti il suo consenso in forma libera e informata, rendendo ancora una volta la tolleranza di "A" legittima.

Il diavolo naturalmente è nei dettagli e, come ammette lo stesso Floridi, all'atto pratico può essere particolarmente difficile definire ciascuna delle tre ipotesi. Si pensi ai casi degli embrioni umani come possibili terzi (ipotesi (i)); o a come determinare la soglia di quanto è "significativo" (ipotesi (ii)); o ai dilemmi, a noi ben noti, del consenso (ipotesi (iii), su cui sopra §§ 5.3.3.1 e 8.2.2). Con le parole del filosofo oxoniense, tuttavia, la soluzione offerta al paradosso della tolleranza "non è un algoritmo da essere applicato meccanicamente. È una regola generale di design normativo che rende possibile l'uso pubblico della ragione nell'applicazione di schemi […] per generare norme concrete. Allo stesso tempo, sarebbe un errore credere che le gravi difficoltà ermeneutiche e argomentative viste ora, sminuiscano il valore della soluzione del paradosso. Al contrario, abbiamo ora una forma per limitare la tolleranza attraverso la tolleranza stessa, senza dover fare rinvio al principio di giustizia".

Tornando di qui alle nozioni di ragione e ragionevolezza informativa veicolate dall'uso del test sull'aspettativa di privacy in Europa, l'aver svincolato il principio di tolleranza dall'omologo della giustizia consente ora di approfondire quanto detto in precedenza, in relazione all'"unica risposta corretta" di Dworkin (§ 9.3.1), al "ragionevole compromesso" di Hart (§ 9.3.2), fino alle quattro leggi morali dell'etica dell'informazione di Floridi (§ 9.3.3). Mentre nel capitolo precedente si è trattato di cominciare a presentare il diritto nella sua miglior forma, in modo moralmente coerente, senza per questo avanzare la pretesa di dedurre da qualche insieme di principi generali la migliore soluzione giuridica per ogni caso, occorre esaminare a continuazione come questi limiti incidano sul principio proprio di tolleranza del test sulla ragionevole aspettativa di privacy.

### 10.4.3. *Giustizia e complessità giuridica*

Abbiamo finora dedicato relativamente poco spazio a uno dei classici temi del diritto, come la giustizia, sia in generale a proposito del riposizionamento tecnologico degli ordinamenti nell'era delle società ICT-dipendenti, sia in particolare sul tema della tutela e protezione della privacy informazionale, per un fondamentale motivo. Esso rimanda ai temi della complessità giuridica, specie nella prima accezione del lemma come comprimibilità algoritmica delle informazioni, introdotto fin dal capitolo secondo (§ 2.1.3). A riprova dell'assunto, basti pensare al rapporto tra le pratiche sociali di una comunità, il ruolo normativo dell'autorità politica e il problema del coordinamento morale tra i consociati, su cui siamo venuti più volte insistendo – da ultimo: § 10.3.3 – in rapporto a due tra le principali famiglie della teoria morale contemporanea; ossia, il deontologismo di Kant e l'utilitarismo di Bentham (su cui § 4.2.2).

Per quanto concerne innanzitutto le teorie risalenti a Kant, l'attenzione si dirige verso la seconda delle sue critiche, quella della "ragion pratica" (1788) e alla *Metafisica dei costumi* (1797). Rispetto alla tradizionale distinzione aristotelica di filosofia teoretica e pratica (v. sopra § 1.1.1), "pratico" rimanda in questo contesto a ciò che

attiene alla determinazione della volontà come opera della ragione e, più in particolar modo, a ciò che è giusto o doveroso fare in ragione dei motivi o intenzioni delle azioni, più che del loro scopo. Come si è richiamato nel capitolo quinto (§ 5.3.3.1), a proposito della variante del contratto sociale in Kant, un primo tipo di dovere è riassunto con la formula dell'imperativo categorico, del dovere per il dovere, di ciò che è giusto fare come fine in sé, sulla base di un nuovo test, quello della cosiddetta universalizzazione: "Agisci unicamente secondo la massima che tu puoi volere ad un tempo che divenga legge universale" (Kant ed. 1969: 72). Il secondo tipo di dovere è invece presentato come un imperativo di tipo ipotetico che detta com'è doveroso agire in vista di un fine, come illustrato dai consigli della prudenza o le regole dell'abilità.

È naturale, dunque, che successivamente sia sorto il problema di appurare quale sia il rapporto, per Kant, tra l'imperativo categorico della morale, su cui è fondato il contratto sociale, e il plesso d'imperativi ipotetici che ritroviamo nella sfera del diritto, come tecnica volta a conseguire il fine della coesistenza degli arbitri individuali (§ 1.1.3). A chi sostiene la tesi della sostanziale connessione tra morale e diritto, si oppongono coloro che, invece, optano per una separazione netta che dipende, in ultima analisi, dal concetto di coazione giuridica: "se A, allora B". Altri, ancora, propendono per un'interpretazione intermedia, nel senso che le due sfere non sono né strettamente connesse, né totalmente separate, dato che la distinzione che Kant pone tra diritto e morale, in ragione della forza coercitiva dei comandi giuridici, è pur sempre basata sul dovere di tutela della dignità umana come fine a sé. Quest'ultima interpretazione precluderebbe la via a quelle letture del pensiero kantiano in chiave formalista e giuspositivistica che, pure, tanta fortuna avrebbero avuto a partire dalla seconda metà dell'Ottocento con il cosiddetto neo-kantismo della scuola di Marburgo che, dal fondatore della stessa, Rudolf Stammler (1856-1938), arriva al giurista più famoso del '900, Hans Kelsen.

Quale che sia l'ermeneutica dei testi kantiani, tuttavia, il complessivo impianto deontologico della sua dottrina male si addice a cogliere la ricchezza del fenomeno giuridico. Sul fronte dell'etica delle intenzioni, basti far caso a tutte le ipotesi di responsabilità giuridica discusse nell'ottavo capitolo (§ 8.5), che poggiano ora sugli effetti concreti – i danni – dei comportamenti tenuti dagli agenti, ora, invece, prescindono del tutto dalla valutazione delle loro finalità, motivi o intenzioni. Sul fronte degli imperativi ipotetici, viceversa, valgono anche nei confronti di Kant, le obiezioni mosse all'allievo neo-kantiano Kelsen, per cui, tanto con gli esempi del diritto soffice (§§ 4.3.1.1, 6.3.2 e 9.1), come con le tecniche dell'"opt in" (§§ 4.3.3.2, 5.3 e 8.3.1), riesce difficile cogliere in nome delle sanzioni dell'ordinamento, molte figure del diritto contemporaneo.

Analoghe considerazioni valgono, sia pure a ranghi rovesciati, per l'altra famiglia delle teorie morali che fanno capo all'utilitarismo benthamiano. Qui, come illustrato con le tesi dell'analisi economica del diritto (§ 8.5), l'accento cade sugli esiti, e non già sui fini o moventi, dell'interazione sociale, per cui le questioni di responsabilità sono affrontate come questione di bilanciamento tra costi e benefici. Agli antipodi dell'universalismo kantiano, è stato così sostenuto che "il ruolo delle entità mentali nel diritto, come accade con l''intenzione', dovrebbe diminuire man mano che il diritto diviene più sofisticato" poiché "nella misura in cui il diritto matura, la respon-

sabilità – perfino quella penale – diventa progressivamente più 'esterna', vale a dire più una questione di condotta, che d'intento" (Posner 1988: 868).

Va da sé che, in maniera eguale e contraria al deontologismo kantiano, anche a questi approcci utilitaristici al diritto sfugge una parte consistente del fenomeno giuridico. Lasciando da parte il ruolo che le intenzioni svolgono nella valutazione che il diritto fa dei comportamenti umani – come avviene nel settore penale, al fine di appurare quali siano eventualmente le aggravanti, o scusanti, del caso – abbiamo visto fattispecie in cui le decisioni degli agenti non solo non sono state dettate dalla minaccia di sanzioni legali ma anche, con buona pace di Posner, sono andate contro i dettami di un'asettica razionalità economica (v. ad esempio § 5.4.2).

Senza addentrarci ulteriormente nelle secche dell'utilitarismo (e deontologismo) applicato alla sfera giuridica, la nostra attenzione si è già soffermata su altre e più rigorose sistemazioni dell'etica che permettono di aggiornare in chiave informativa le basi del costituzionalismo moderno imperniato sull'idea di contratto sociale e che, in questo modo, consentono di affrontare su più solide basi le sfide giuridiche poste dalla rivoluzione tecnologica. Nel capitolo nono, è stata richiamata in questa direzione l'etica dell'informazione di Floridi (§ 9.3.3). Pure in questo caso, però, anche a seguire le leggi morali formulate dal filosofo oxoniense, dovremmo tenere presente di come, prima o poi, finiremo per incontrare alcuni bivi dell'argomentazione giuridica, per i quali le difficoltà, o "casi difficili", in cui va a parare di tanto in tanto l'ordinamento, richiedono decisioni e compromessi in sede politica, più che considerazioni di stretto diritto. Se ne è fatto cenno con il disaccordo che verte ora sui principi giuridici di riferimento, ora sui concetti in gioco, ora sul diverso modo in cui tali concetti sono correlati (§ 9.3.2). La conclusione da trarsi è stata quella per l'appunto sviluppata nelle pagine del presente capitolo, e sempre sulla scia delle indicazioni di Floridi, a proposito del principio di tolleranza. Stante i fenomeni d'incompletezza che segnano il linguaggio che ha di mira il mondo del diritto, per via della sua stessa specifica complessità, si è dovuto "raffrontare in qualche modo il proprio giudizio nei limiti della complessiva ragione umana", usando la terminologia di Kant.

In sostanza, lo spirito di tolleranza matura proprio in ragione dei limiti delle leggi e principi, che dovrebbero orientare e condurre l'interazione umana. Il punto lo si è già evidenziato in rapporto all'esportabilità del test sulla ragionevole aspettativa di privacy in Europa, a partire dalla sfera dove la discrezionalità del giudizio dovrebbe essere minore rispetto al settore della produzione delle leggi, vale a dire l'ambito della loro applicazione da parte dei giudici (§ 10.3.1). Nonostante la generalità e astrattezza dei principi che si è tenuti a far valere nei casi difficili del diritto, tanto in sede giurisprudenziale come, a maggior ragione, in sede legislativa, bisogna però trovare il modo per testare la bontà dei compromessi che, al modo di Hart (§ 9.3.2), si rendono necessari nei termini di una ragionevolezza informativa. Davanti ai bivi o diramazioni in cui va a parare di tanto in tanto l'argomentazione giuridica, è qui che entra in campo la seconda accezione del termine "tolleranza" cui si è fatto cenno in precedenza. Al fine di venire a capo dei casi difficili del diritto, occorre infatti prendere atto di qualsiasi differenza tra ciò che è fissato dai principi dell'ordinamento e la loro realizzazione effettiva, entro lo scarto definito dai principi e criteri di una teoria moralmente coerente, come l'etica dell'informazione di Flo-

ridi. Sebbene quest'ultima non possa garantire l'algoritmo che consenta di pervenire all'unica risposta corretta per ogni caso giuridico, essa può fondare la ragionevolezza dei compromessi resi necessari dall'incompletezza dell'ordinamento. Si tratta di precisare su queste basi i limiti di una tollerabile indeterminatezza.

### 10.4.4. *Tolleranza e complessità giuridica*

L'insufficienza dei parametri di giustizia da cui trae conferma il ruolo autonomo che la tolleranza svolge nel sistema giuridico, non significa abbracciare il nichilismo o, quanto meno, approdare a esiti formalistici. A ciò ostano sia motivi di tipo processuale e latamente formale, sia ragioni sostanziali o di contenuto, che siamo venuti esponendo nel corso di queste pagine. Per comodità, riepiloghiamo le varie tappe che hanno condotto fino al punto di declinare i temi della complessità in termini di tolleranza.

Innanzitutto, sul piano formale, bisogna ribadire come siano costitutivi del principio giuridico di giustizia, ricondotto al criterio della terzietà di chi giudica, alcuni parametri come l'equidistanza e disinteresse rispetto alle parti in causa (§ 10.4.2). Ciò significa che, nel decidere delle ragioni di "A" e "B", "C" deve confermare il suo giudizio anche a parti rovesciate, salvo poi dover rinunciare al proprio mandato, come accaduto a *justice* Marshall nel caso Katz (§ 7.2.2), per conflitto d'interesse. Si tratta delle condizioni non funzionali che definiscono l'architettura del sistema, vale a dire ciò che l'ordinamento si suppone debba essere. Come tali, dette condizioni si applicano anche alla funzione legislativa, la quale può essere convenientemente presentata come pubblica, non contraddittoria, comprensibile e non effimera (Fuller 1969). Questi requisiti vanno a loro volta integrati con le componenti funzionali del sistema, ossia, ciò che definisce come l'ordinamento operi, piuttosto che il suo modo di essere. Tra i requisiti funzionali, si pensi nuovamente al ruolo informativo delle leggi e delle sentenze nel sistema giuridico, assunte come messaggi che veicolano una determinata informazione sulle norme in questione (§ 2.1.2.1). Questa funzione, va da sé, ha pure un compito ermeneutico e pragmatico, nel senso d'interpretare se stessa e l'ambiente sociale che la informa, al fine di precisare l'insieme di regole o istruzioni, che determinano il modo di essere di altre entità. È quanto, nel capitolo secondo, si è riassunto come "informazione per la realtà", IPR o Info2 (§ 2.1).

Tuttavia, si è anche visto come questa duplice funzione ermeneutica e pragmatica del diritto possa dar luogo a controversie, a volte sul piano del significato e natura dei principi giuridici del sistema, in altri casi dei termini e forme dell'argomentazione. Di qui che, su un piano strettamente processuale, sia stata introdotta un'ulteriore serie di accorgimenti, nella dimensione dell'onere probatorio e con il dovere di conoscenza che entra in campo con la scelta degli strumenti normativi (§ 3.4.3). Mentre, nel capitolo terzo, gli esempi sono venuti dai problemi della governance d'internet, nel capitolo precedente l'attenzione si è invece soffermata sulle analoghe scansioni processuali dell'odierno dibattito sulla riforma della direttiva europea in tema di dati personali (§ 9.1). Sul piano filosofico, simili criteri sono stati ripresi, e ulteriormente raffinati, in rapporto alle riflessioni kantiane sulla critica del giudizio riportate nel presente capitolo.

Dal punto di vista sostanziale, abbiamo infine riferito come, pure a cogliere la

funzione ermeneutica e pragmatica del diritto in maniera moralmente coerente, al fine di garantire o preservare l'integrità della legge al modo di Dworkin, ci sia talora bisogno di venire a capo dei problemi dell'ordinamento tramite un compromesso ragionevole (§ 9.3.2). Qui, come riferito nello scorso paragrafo, l'aiuto che una teoria moralmente coerente offre al giurista, come avviene con l'etica dell'informazione di Floridi, è di precisare lo scarto massimo ammissibile tra ciò che è stato fissato astrattamente dalle norme del sistema – o dal conflitto tra i principi e norme di più sistemi – e il grado della loro realizzazione effettiva in una circostanza determinata. Si tratta della seconda accezione di tolleranza cui abbiamo fatto prima riferimento e che, nell'era delle società ICT-dipendenti, consiglia di prestare nuovamente attenzione al livello di astrazione che coglie gli oggetti dell'analisi in termini informazionali (§§ 1.4 e 9.3.3). Per delimitare lo scarto massimo ammissibile ai fini della ragionevolezza dei compromessi resi necessari dai casi difficili del diritto, bisognerà appurare innanzitutto se sia possibile prevenire ogni forma d'impoverimento dell'essere, o entropia, nell'infosfera; ossia, ogni tipo di distruzione o corruzione di oggetti informazionali. Tanto più ragionevole sarà il compromesso, quanto meno entropia sia richiesta, sia prevenendone la creazione, sia rimuovendola dall'ambiente, oppure preservando, coltivando, aumentando o arricchendo al tempo stesso le proprietà del sistema e dei suoi oggetti.

A continuazione, occorre appurare come questi margini di ragionevole tolleranza operino nel concreto del test sulla ragionevole aspettativa di privacy informazionale. Definiti i termini in cui si può propriamente parlare di ragionevolezza giuridica, bisogna infatti individuare il nesso tra i casi difficili del diritto e le pretese normative dei consociati, seguendo del resto l'ispirazione originaria del test ideato dal giudice Harlan nel caso Katz. Davanti alla fitta rete di disposizioni normative, sentenze e opinioni che vigono oggi in Europa, si tratta di far sì che anche i cittadini possano orientarsi in materia di privacy e protezione dati. Per gettare un ponte tra *taxis* e *kosmos*, in che modo, dunque, tarare il test in Europa? Come sfruttarne la specifica tolleranza?

## 10.5. *La prova del test*

La prova di un test e, con questa, il suo risultato dipendono ovviamente dal tipo di esperimento condotto, o dal modo in cui quest'ultimo è congegnato. Nel primo caso, la risposta potrà essere binaria, si/no, come nel caso del test di gravidanza; oppure, condurre alla quantificazione di un responso, come avviene con i test d'intelligenza o quelli attitudinali. Nel secondo caso, il tipo d'informazione varierà a seconda dell'impostazione del test, come emerso proprio in rapporto al test sulla ragionevole aspettativa di privacy. La prova potrà infatti essere condotta attraverso una serie di domande per accertare l'attendibilità di certe opinioni, tramite rilevazioni statistiche per campioni come quelle condotte dalle indagini a cura dell'Eurobarometro (§ 10.3.2); oppure, in chiave normativa, per mettere in mostra cosa gli individui pretendono sia loro tutelato. Quest'ultimo è stato il livello dell'analisi svolta fin qui nel capitolo, al pari di come il test sulla ragionevole aspettativa di privacy è impiegato del resto nel suo paese d'origine, gli Stati Uniti.

Al fine di procurare l'efficacia del test in un sistema giuridico diverso come quello europeo, si è reso tuttavia necessario precisare ulteriormente i termini della questione da chiedere tramite il test. Rispetto alla domanda originaria, relativa alla tutela che i cittadini americani hanno rispetto alle indagini del proprio governo, o stato, in nome del Quarto emendamento, nella sua variante europea il test è stato tarato nei termini della privacy informazionale, ossia nei termini elementari dell'opacità degli individui, come gradi di frizione ontologica tra agente e sistema, individuo e società (§§ 9.4.3 e 10.1).

Successivamente, si è provveduto a predisporre le ulteriori condizioni di trapianto giuridico, nella consapevolezza che queste operazioni possono dar luogo a vere e proprie crisi di rigetto. Avendo a mente le differenze, anche profonde e sostanziali, tra i modelli statunitense ed europeo della protezione dati e della privacy, si è pensato così al test di Katz come un banco di prova critico, sulla cui base valutare l'azione del gubernaculum, vale a dire le decisioni politiche dei legislatori, quanto quelle dei giudici (§ 10.2).

In modo ulteriore, si è ristretto il banco di prova del test, escludendo dallo stesso l'insieme di principi che formano la prima direttiva comunitaria in tema di protezione dei dati. La ragione è dipesa dal fatto che la ragionevole aspettativa di privacy informazionale esistente oggi in Europa, è maturata proprio grazie ai principi di questa direttiva che, per ciò stesso, tenuto conto della velocità del progresso tecnologico, fungono da parametro per valutare la legislazione successiva e, in senso kantiano, anche ogni normativa futura (§ 10.3).

Infine, si è provveduto a fornire gli elementi del caso per tarare il test con un certo margine di tolleranza, definendo uno scarto massimo ammissibile tra i principi della aspettativa, o pretesa, e la loro realizzazione effettiva. Nel paragrafo precedente, questo accorgimento è parso necessario in rapporto alla risoluzione dei casi difficili del diritto, con i ragionevoli compromessi che ne derivano: qui, il margine di tolleranza risulta opportuno per un ulteriore motivo. Al modo di altri test in ambito giuridico e normativo, come i test di Kant sulla ragionevolezza di ogni legislazione pubblica, o sull'universalità delle massime dell'agire, tale accorgimento sulla ragionevole indeterminatezza del test consente infatti di tararlo in modo tale, da avere ancora una volta come risposta un sì o un no.

Per comodità del lettore, la messa a punto del test è compendiata con l'ultima figura di questo capitolo e del libro:


Figura 30: *Una ragionevole aspettativa in Europa.*

Sulla base delle quattro componenti del test in chiave europea, compendiate dalla figura 30, è dato chiarirne, per così dire, la quintessenza. La privacy informazio-

nale degli individui si profila, sempre di più, come punto nevralgico dell'ordinamento, crocevia di settori cruciali come la sicurezza nazionale e l'ordine pubblico, la libertà di parola e di pensiero, il diritto di cronaca e all'informazione, il riuso delle informazioni del settore pubblico e la tutela della proprietà intellettuale, oltre alla tradizionale protezione relativa alla riservatezza e all'identità personale, contro gli atti diffamatori, la diffusione dei fatti privati o la loro distorsione sotto falsa luce.

Eppure, nonostante la criticità dell'istituto, spesso è impossibile per gli individui orientarsi nel dedalo di disposizioni, leggi e sentenze, opinioni e raccomandazioni che, a stretto rigore del formalismo giuridico, dovrebbero definire la pretesa delle parti. Nel paese d'origine del test, esso ha il ruolo encomiabile di fare da ponte tra taxis e kosmos, gubernaculum e norme sociali. In Europa, sia pure nei limiti precisati nel presente capitolo, il test dovrebbe svolgere una funzione analoga, rispetto sia alle decisioni delle autorità politiche e giuridiche, sia in vista delle nuove sfide che la tecnologia è pronta a proporre.

Ritiene il lettore che la sua aspettativa di privacy sia ragionevolmente difesa?

### 10.5.1. *Tre esempi e un corollario*

Proviamo a chiarire ora con tre esempi, le implicazioni del test: a confronto con chi dovrebbero esserne, in fin dei conti, i beneficiari con la loro ragionevole aspettativa di privacy, i possibili candidati oggetto del test sono sia le decisioni del gubernaculum, sia quelle della iurisdictio, a confronto con le tre dimensioni tipiche del settore. Il richiamo va ancora una volta alla privacy in luogo pubblico (§§ 7.2.2 e 9.4.1), a quella domestica (§§ 7.3.1 e 9.4.2), e alla loro convergenza nelle odierne società ICT-dipendenti, ossia, la cosiddetta infosfera o esperienza onlife (§§ 7.4 e 9.4.3).

I tre esempi riprendono casi in parte già discussi: i "pedinamenti digitali" in Italia (§ 9.4.1); gli obblighi di cancellazione dei dati degli ISP (§ 9.2.3); e le nuove sfide alla privacy informazionale poste dall'autonomia degli agenti artificiali (§ 9.4.2). La ragione dipende dal fatto che questi problemi di tutela sono destinati a riproporsi in forme nuove a breve.

#### 10.5.1.1. *Pedinamenti digitali*

Uno degli aspetti più eclatanti della rivoluzione tecnologica non consiste solo nel creare, com'è evidente, nuovi casi e fattispecie che sarebbero semplicemente impensabili o impossibili senza la tecnologia di riferimento; ma, nel trasfigurare e piegare a sé casi e fattispecie ereditati dalla tradizione. Così, è chiaro che la firma elettronica non sia un modo di rinverdire la consueta figura della sottoscrizione, la tutela digitale del copyright non è una forma di aggiornare il vecchio diritto d'autore, la notifica telematica un mezzo per svecchiare le mansioni degli ufficiali giudiziari o, con buona pace della Corte di cassazione in Italia o *justice* Scalia a Washington, l'impiego del GPS e la ripresa di "immagini non comunicative" da parte delle forze dell'ordine un modo semplicemente più scaltro per pedinare le persone. Abbiamo visto, infatti, che attraverso l'uso del GPS si può fare con minimo sforzo e costi economici irrilevanti ciò che, fino a poco tempo fa, avrebbe richiesto il coordinamento di

un'intera squadra di agenti pedinatori, con riprese video e magari l'uso di elicotteri, per tenere sotto controllo i movimenti di una persona, ventiquattro ore su ventiquattro (v. § 7.4).

Questo scenario, va da sé, è destinato a ripresentarsi in forma esponenziale, nel senso che alla visione profetica di Brandeis nel 1928, per cui "il progresso della scienza nel fornire al governo gli strumenti di spionaggio non si fermerà certo all'uso delle intercettazioni telefoniche" (§ 7.2.1), è sufficiente innestare la potenza geometrica della legge di Moore (§ 1.3). Mentre, nel capitolo sesto, ci siamo occupati dei profili tecno-filosofici del problema con i temi della morte della privacy e il risorgere dell'araba fenice, qui, invece, conviene testare il nostro metodo con l'orientamento fin qui accolto dalla Suprema di Roma. Nel capitolo precedente, richiamando le note critiche di Monica Senor (§ 9.4.1), si è avuto modo di segnalare come la Cassazione ha pensato bene di rubricare la protezione della privacy informazionale sulla base dell'articolo 2 della Costituzione, per cui detta tutela è priva delle garanzie previste dalla doppia riserva di legge e di giurisdizione che è, viceversa, accordata dall'articolo 14 all'"inviolabilità" del domicilio. È ciò ragionevole?

Naturalmente no, nel senso che anche in Italia, per dirla con *justice* Harlan, "la società è pronta a riconoscere come ragionevole" l'aspettativa che uno non sia pedinato digitalmente senza le garanzie e i controlli di un'autorità indipendente. Sul piano formale, molti invocano una revisione costituzionale che recepisca formalmente in Italia il quadro di tutela previsto dall'*habeas data* europeo (§ 8.1.4). Per intanto, basterebbe però recepire il buon senso dettato dal test di Katz, integrando la lettura dell'articolo 2 con l'articolo 8(3) della Carta europea dei diritti fondamentali. È chiedere troppo alla Cassazione?

### 10.5.1.2. *Obblighi di cancellazione*

La seconda classe di liti su cui esercitare la prova del test, riguarda il vigente articolo 6(e) D-95/46/CE sulla conservazione dei dati, come interpretato dalla Corte di Lussemburgo in *Costeja González vs. Google* (§ 8.5.2.2); quadro normativo sul quale andrà a innestarsi il nuovo diritto alla cancellazione, su cui Commissione e Parlamento europei troveranno l'accordo ai sensi del nuovo articolo 17 del regolamento (v. § 9.2.3). Lo scenario prevede alcuni individui che pretenderanno di esercitare il proprio diritto "di ottenere dal responsabile la cancellazione dei dati personali che li riguardano e astenersi dall'ulteriore disseminazione di quei dati, e di ottenere da terzi la cancellazione di ogni collegamento, copia o replica di quei dati". Sebbene tale pretesa trovi dei limiti, tra cui la libertà di parola dei terzi interessati, è ragionevole attendersi che questi ultimi ottemperino al nuovo obbligo? Dopo il secolo della memoria, il ventesimo, per caso diventerà il ventunesimo secolo, almeno in Europa, il secolo del diritto all'oblio?

Rovesciando i termini di *justice* Harlan, è da prevedere che "la società non sarà pronta a riconoscere come ragionevole" simile aspettativa come regola generale di condotta. A ciò osta, innanzitutto, il fatto che la memoria individuale, mediante la quale si attribuisce un significato al proprio passato – magari attraverso la cancellazione dei dati personali – non è mai un gioco privato, ma presuppone invece la dimensione sociale che dota di senso quello stesso ricordo. Per dirla con un profondo

conoscitore di questi temi, "il primo fatto, il più importante, è che non ci si ricorda da soli, ma con l'aiuto dei ricordi altrui. Inoltre i nostri pretesi ricordi sono molto spesso presi in prestito da racconti sentiti da altri. Infine, e questo è il punto decisivo, i nostri ricordi sono inquadrati in racconti collettivi" (Ricouer 2004: 54). All'atto pratico, molti dei sedicenti "dati personali" sfuggono infatti alla pretesa proprietaria del titolare dei dati, perché ora nascono dalla relazione con gli altri, ora sono costitutivamente condivisi con terzi o, soprattutto, perché il potere di ricostruzione del passato deve saper convivere con il potere che gli altri hanno di accedere alla conoscenza delle tracce di quel passato. È in questi termini che si basa in fondo quella condivisione della conoscenza che è essenziale alla formazione del sapere e alla costruzione di un mondo dotato di significato.

La dimensione sociale o collettiva in cui va dunque inscritto ogni sedicente diritto all'oblio non significa, ovviamente, che l'oblio non svolga un ruolo, perfino cruciale, nella esperienza umana (Pagallo e Durante 2013; 2014).

Ma, sul piano giuridico, saranno le norme sociali, più che l'astratto dettame del legislatore o dei giudici, a determinare il modo in cui la pretesa soggettiva ad essere dimenticati tramite il diritto alla cancellazione dei dati, verrà concretamente bilanciata con gli altrui diritti al ricordo, alla libertà di parola e, in genere, all'interesse pubblico all'informazione e alla conoscenza. Sul piano formale, la questione finirà per ruotare attorno all'articolo 17.3(a) del nuovo regolamento come punto di equilibrio per simile bilanciamento. Sapranno le istituzioni europee apprendere dai propri errori, applicando a se stesse il test di Katz?

#### 10.5.1.3. *Autonomia artificiale*

L'ultimo esempio del test riporta ai rapporti che, di qui a breve, intesseremo con agenti artificiali "intelligenti" e "autonomi", nel senso specificato nel capitolo precedente (§ 9.4.2). Mancando del tutto ogni referente giurisprudenziale e normativo, qui il test non può che vertere su ciò che gli individui pretenderanno ragionevolmente dalle autorità del futuro, vale a dire preservare l'integrità di quell'insieme discreto e ben strutturato di dati, secondo cui l'identità degli individui può essere convenientemente rappresentata, alla luce dei gradi di "frizione ontologica" tra agente e sistema, individuo e società (§§ 9.4.3 e 10.1). Questa ragionevole aspettativa dei consociati, da un lato, comporta la pretesa che le autorità pubbliche consentano d'introdurre simili applicazioni robotiche nell'ambito domestico, soltanto quando esse saranno in grado di rispettare la distinzione tra trasparenza nell'elaborazione dei dati e relativa opacità degli interlocutori umani. Si tratta, come detto, di uno dei settori più vibranti e dinamici dell'odierna ricerca sull'intelligenza artificiale e della privacy tramite design, avendo il fine di immettere questo tipo d'informazione nei programmi degli agenti artificiali affinché questi ultimi si regolino di conseguenza (§§ 9.2.5 e 9.4.2).

D'altro canto, però, abbiamo anche visto come i gradi di frizione ontologica che orienteranno il comportamento degli agenti artificiali, dipenderanno in buona parte dalla loro stessa interazione con gli uomini come propri "badanti". Questo non soltanto vuol dire che lo stesso modello di robot finirà per comportarsi diversamente, dopo poche settimane o giorni, a seconda di come gli individui abbiano trattato il

proprio agente artificiale. In realtà, l'imprevedibilità degli esiti cui potrà dar luogo la nuova interazione tra uomini e robot, è destinata a riplasmare le accezioni fin qui viste della privacy, dato che i termini della non intrusione o esclusione, della limitazione, accesso o controllo, andranno riferiti all'autonomia degli agenti artificiali, più che a quella di altri esseri umani. Dal punto di vista della ragionevole aspettativa di privacy, il rischio è che gli ordinamenti possano correre ai ripari con nuove forme di paternalismo, in modo cioè da difendere gli individui dalle loro stesse inconsulte decisioni (§ 5.3.3). Una forma per prevenire simile scenario, nondimeno, esiste; ed è di spostare il fulcro del sistema dal consenso del titolare dei dati, ai rischi derivanti dall'uso di quei dati. Si tratta di una tesi svolta nel corso delle pagine precedenti, proprio al fine di venire incontro al riposizionamento tecnologico dell'istituto (v. §§ 8.4 e 9.2.2).

#### 10.5.1.4. *Il corollario*

Il delicato equilibrio tra norme sociali, gubernaculum e iurisdictio, su cui siamo venuti insistendo in queste pagine sulla ragionevole aspettativa di privacy, non concerne solo quest'ultimo e sia pur importante settore dell'ordinamento giuridico. Il tema ha anzi rappresentato uno dei fili conduttori dell'intero libro, a partire dalle annotazioni di Hayek su kosmos e ordini spontanei (§ 2.2); per giungere al ruolo delle consuetudini nell'odierno sistema delle fonti (§ 4.2.3 e tavola 6 in § 4.3.3.2); fino ai problemi di fattibilità del design istituzionale e delle norme (§§ 5.1.3 e 5.4.2). La ragione dell'interesse è dipesa da un duplice ordine di fattori.

Il primo concerne il piano specifico dell'odierna tutela della privacy informazionale: il diverso ruolo che le norme sociali e le leggi formali, le fonti fatto e le fonti atto, gli ordini spontanei e la programmazione politica svolgono sul piano dell'esercizio dei diritti e della loro stessa tutela, ha infatti consentito di gettare luce sui diversi modelli, statunitense ed europeo, dell'istituto. Al ruolo determinante che le forze del mercato e l'autonomia individuale hanno non di rado nel sistema americano, fa da controcanto il potere normativo dell'"effetto Bruxelles", sia pure temperato dalle regole sul consenso individuale e con modalità di auto-regolazione, come avviene con i codici di condotta; oltre alle forme di diritto soffice, come nel caso dei poteri assegnati alle autorità garanti indipendenti; fino alle aperture del modello all'esperienza maturata in altri sistemi giuridici, o con strumenti di cooperazione internazionale e transnazionale. Anche a seguire i critici dell'approccio dall'"alto verso il basso" proposto dal modello di Bruxelles, bisogna dunque ammettere che quest'ultimo lascia un qualche spazio all'autonomia individuale, alle norme e pratiche sociali. Per rafforzare e consolidare questo spazio, lo scopo di questo capitolo è stato di mostrare come, sia pure a determinate condizioni, il test sulla ragionevole aspettativa di privacy sia applicabile anche in Europa.

Per quanto concerne invece il piano generale dell'analisi, il rapporto tra norme sociali e leggi formali, tra fonti fatto e fonti atto, tra ordini spontanei e programmazione politica, ha offerto l'ulteriore possibilità di approfondire struttura e dinamiche dei sistemi giuridici. Sul piano strutturale, si è già detto più volte che il luogo dell'autorità politica, tanto a Bruxelles quanto a Washington, non va collocato in una sorta di vuoto normativo; ma, piuttosto, sia da ricondurre alle convenzioni e usi

sociali tesi a risolvere il problema del coordinamento morale tra i consociati. Sul piano teorico, sulla scorta delle indicazioni di Kant e sia pure di quelle estetiche sul gusto, si è così precisato nel corso di quest'ultimo capitolo, come intendere questa riconduzione delle autorità politiche e giuridiche, e cioè sia del gubernaculum che della iurisdictio, alle pratiche sociali, nel duplice senso di una critica del giudizio e come prolegomeni a ogni legislazione futura (§§ 10.3.2 e 3). Il richiamo di Kant ai "limiti della complessiva ragione umana" è servito, anche contro le sue stesse intenzioni, a declinarne il concetto più in chiave di tolleranza, che di giustizia.

Tuttavia, a prevenire ciò che un fiero critico di Kant, ossia il filosofo tedesco G.W.F. Hegel (1770-1831), liquidava come "intelletto astratto", occorre ricordare come, nel corso dei secoli, sia venuto mutando questo modo di concepire il compito che la legge ha di trasmettere la propria autorità alla struttura sociale di riferimento. Dal pluralismo medioevale (§ 4.2.1), si è passati al monismo legislativo del modello di Westfalia (§ 4.2.2), fino all'odierno assetto delle società ICT-dipendenti con le nuove forme di governance e del diritto transnazionale (§ 4.3.3.2). L'esame dei temi della privacy e con la tutela dei dati personali ha non solo confermato come la complessità dei sistemi giuridici sia venuta crescendo con l'incidere dell'impatto tecnologico; ma ha del pari ribadito quanto osservato in sede storica (§§ 4.3, 4.3.2.1, 4.3.3.3 e 5.4), e cioè che il riposizionamento delle fonti del diritto sia legato a questioni di potere (§ 9.2.4). Mentre, nel presente capitolo, l'idea è stata di chiarire sulla scorta di un test, molti dei dilemmi che segnano la privacy al giorno d'oggi, non bisogna per ciò dimenticare il quadro generale, entro cui situare questi stessi problemi. Tra l'apparente semplicità del test e la complessità dei mutamenti in atto, occorre tirare le fila del discorso con le conclusioni del libro.

# *Conclusioni*

"Nulla di grande è stato mai compiuto al mondo senza passione"
G.W.F. HEGEL

Le conclusioni di una ricerca sono canonicamente volte a presentarne i risultati, sulla base di un quadro d'assieme dal quale, possibilmente, trarre un messaggio. È la "t-shirt" menzionata nel capitolo quinto, a proposito del design della comunicazione (§ 5.1.3). Assecondando la tradizione, scandiamo il discorso in ragione di tre obiettivi principali: essi mirano a compendiare i risultati fin qui raggiunti, per chiarire i problemi rimasti sul tappeto e, alla luce di questi ultimi, delucidare ciò che rappresenterà in fondo il succo dell'indagine, il suo messaggio.

*****

L'indagine sul diritto nell'era delle società ICT-dipendenti ha messo in mostra il riposizionamento tecnologico degli ordinamenti giuridici contemporanei su tre piani; vale a dire, quelli relativi alla governance, alle fonti del diritto e al design istituzionale e delle norme. Il terzo capitolo del libro si è così occupato del passaggio dalle tradizionali forme di governo a quelle dell'odierna governance, per cui l'apparato degli stati nazionali è stato più spesso affiancato, e in molti casi sostituito, da un complesso reticolo istituzionale. Questo reticolo è composto da attori sia privati che pubblici, spesso sul piano internazionale e transnazionale, attraverso il quale le decisioni sono prese e l'autorità viene esercitata in un ordinamento determinato. La figura 15 in § 3.3 è servita a illustrare questo primo piano del riposizionamento giuridico.

Secondariamente, nel capitolo quarto, l'analisi ha avuto a oggetto la statica, più che la dinamica, dei mutamenti in corso, vale a dire il nuovo sistema delle fonti nelle società ICT-dipendenti. Alla semplicità del modello di Westfalia, monista sul fronte interno e dualista in chiave internazionale, ha fatto séguito un sistema pluralista e spiccatamente policentrico, il quale, da un lato, aggiunge alla dicotomia tra diritto nazionale e diritto internazionale, la nuova dimensione del diritto transnazionale; e, d'altro canto, integra la dialettica tra gubernaculum e iurisdictio con le forze del kosmos, tra contratti e norme sociali. La tavola 6 del § 4.3.3.2 riassume il nuovo sistema di riferimento sul fronte dei fattori di produzione giuridica dell'ordinamento.

Infine, nel capitolo quinto, l'attenzione è andata agli ambiti, finalità e problemi del design, per chiarire come le regole del diritto vengano ora immesse più spesso negli ambienti, spazi e oggetti che mediano l'interazione dei soggetti. L'idea alla ba-

se del design giuridico è in fondo di affrontare i problemi posti dall'innovazione tecnologica, come nel caso dei conflitti di competenza e di giurisdizione nello spazio transfrontaliero d'internet, per mezzo della tecnologia stessa. Alla canonica rappresentazione del diritto come mezzo di controllo sociale che si avvale della minaccia di sanzioni fisiche, si affianca in questo modo l'idea di un'attuazione del diritto in forma automatica. La figura 17 del § 5.3 compendia il nuovo insieme di problemi e questioni specifiche che il design giuridico solleva in questo modo al giorno d'oggi.

Alla luce di questo quadro generale, la seconda parte del libro è stata dedicata a un settore particolare del diritto, quale quello della privacy e del regime di tutela dei dati personali. La scelta è dipesa dalla rilevanza che questi istituti hanno nell'era delle società ICT-dipendenti, trattandosi di una sorta d'interfaccia tra un principio chiave del diritto, relativo alla sicurezza nazionale e all'ordine pubblico, e le forme in cui i restanti diritti e interessi individuali sono protetti all'interno dell'ordinamento. Mettendo a confronto come questa sorta d'interfaccia operi nel concreto dei sistemi giuridici degli Stati Uniti d'America e dell'Unione europea, si è avuto modo di delucidare come il quadro d'assieme emerso nella prima parte del volume, su governance, fonti del diritto e design, si configuri in questo settore dell'ordinamento. Tra le particolarità, basti qui accennare a quanto, nel capitolo nono, si è riassunto come "effetto Bruxelles", vale a dire il caso, per certi versi unico nell'odierno panorama delle fonti, per cui il potere regolativo di un singolo attore della governance mondiale finisce per influenzare unilateralmente gli altri stati, le organizzazioni internazionali e le forze del mercato (§ 9.1).

L'effetto Bruxelles serve del resto a rimarcare ciò che si è ripetutamente osservato nel corso del volume e, cioè, che il riposizionamento del diritto nell'era delle società ICT-dipendenti non può che comportare questioni di potere. Si è trattato infatti di uno dei fili conduttori dell'indagine, tanto sul piano della teoria del diritto e, più in generale, sul fronte dell'evoluzione umana, quanto nello specifico ambito della privacy informazionale. Non è certo per caso che il capitolo primo abbia preso le mosse dalla lotta tra gli ominidi nell'Africa di quattro milioni d'anni or sono! A partire dalle tesi del sofista Trasimaco sulla giustizia come l'utile del più forte (§ 1.1.2), si è passati alle idee di Hobbes sullo stato di natura e i poteri del sovrano derivanti dal contratto sociale (§ 2.1.2.1); proseguendo con il giusnaturalismo di Locke (§ 3.1.1), e la democrazia di Rousseau (§ 3.1.2); fino al disegno istituzionale dei padri fondatori americani di contrastare il potere con il potere (§ 3.1.3.1), secondo temi e motivi che hanno condotto alle sfide giuridiche dei giorni nostri. Per ciascuno dei piani in cui il riposizionamento tecnologico del diritto è stato acclarato, tra governance, fonti e design, un analogo fenomeno di ridistribuzione e contesa sul potere è stato individuato di conseguenza.

Sul piano istituzionale, nel passaggio dal governo alla governance (§§ 3.3, 3.4.2.1 e 4.3.3.3), l'esempio più chiaro di questa contesa è venuto dall'odierno dibattito sui poteri regolatori d'ICANN e, più in generale, dalla discussione sulle sorti d'internet. Lasciando da parte le scelte di stati autoritari come la Cina, è significativo che i governi di molte democrazie occidentali covino al giorno d'oggi la speranza di porre finalmente i diversi livelli della rete sotto lo stretto controllo degli stati.

Sul piano delle fonti, tra taxis e kosmos (§§ 1.4.3, 4.3.2.1 e 2), si pensi invece alla possibilità di scelta che gli individui hanno tra ordinamenti diversi – ciò che, prima

dell'era di internet, era appannaggio quasi esclusivo delle imprese multinazionali – e a come il rapporto tra il diritto transnazionale di queste stesse società e il diritto nazionale degli stati abbia, talora, condotto alla denuncia dell'odierna *lex mercatoria* come una sorta di nuovo imperialismo giuridico che accentua la contrapposizione tra il "nord" e il "sud" del pianeta.

Sul piano di attuazione delle leggi, in termini di design (§§ 5.2.3 e 5.4), il caso di scuola è dato infine dai rischi di paternalismo sottesi all'implementazione di dispositivi tecnologici volti al condizionamento o controllo del comportamento umano. All'intento dichiarato di prevenire il verificarsi di eventi presuntamente dannosi o le condotte indesiderate degli individui, si oppongono gli opportuni contro-dispositivi tecnologici che trovano terreno fertile tra i membri di una comunità che, spesso, ritiene la regola stabilita dal legislatore frutto della mala fede o ignoranza.

Analoghe considerazioni, del resto, sono valse per il riposizionamento del diritto in chiave di privacy informazionale e con la tutela dei dati personali. Questioni di potere sono emerse, sul piano della governance, tra Stati Uniti ed Europa, con il "nuovo insieme di problemi" sollevati dalla gestione dei dati commerciali ai fini della sicurezza nazionale (§ 8.4.4). Sul piano delle fonti, sono i conflitti di giurisdizione emersi con le disavventure di Google sul fronte della tutela dei dati in Europa (§§ 6.2.4, 6.3.1 e 8.5.2.2); o, con le diatribe emerse all'interno del diritto dell'UE su a chi spetti l'ultima parola tra Commissione e Parlamento europeo (§ 9.2.4). Mentre, a proposito della privacy tramite design, sono indicativi i dubbi che rimangono anche dopo gli emendamenti presentati dal Parlamento europeo alla proposta di regolamento della Commissione (§ 9.2.5), si tratta in fondo di un tema che appare come l'altra faccia della stessa medaglia su cui si è insistito a lungo nel capitolo decimo, relativamente al bilanciamento tra norme sociali, gubernaculum e iurisdictio (§ 10.5.1.4). Il fatto che le decisioni dell'autorità politica non siano da collocare in una sorta di vuoto normativo, ma vadano piuttosto ricondotte alle convenzioni e pratiche sociali tese a risolvere il problema del coordinamento morale tra i consociati, solleva in definitiva una questione di potere. Come tale, il tema merita di essere ripreso a parte in queste conclusioni.

*****

Alla luce della distinzione introdotta nel capitolo secondo, tra il diritto come informazione "per la realtà" e "sulla realtà" (v. § 2.1), muoviamo innanzitutto da questi livelli d'astrazione che consentono di affrontare le questioni di redistribuzione del potere nell'ambito del diritto.

Il primo livello è dunque quello normativo, concependo cioè l'informazione giuridica come insieme di regole e d'istruzioni per determinare il modo di essere di altre entità: l'informazione giuridica "per" la realtà. È questo il livello di astrazione assunto nella parte generale del volume, quando si sono affrontati i nodi della redistribuzione del potere relativi alla governance d'internet. I criteri normativi introdotti in quella sede, come si ricorderà (§ 3.4.3), hanno fatto leva sui meccanismi processuali del diritto in termini dell'onere della prova e del dovere di conoscenza che si ha al fine della scelta degli strumenti normativi. Altri esempi di come operino nel concreto questi criteri in chiave processuale sono stati visti, tanto in rapporto

alla neutralità tecnologica delle scelte giuridiche (§ 5.3.1), come con la proposta di regolamento sulla tutela dei dati presentata dalla Commissione europea nel 2012 (§ 9.1); come pure, infine, con le ragioni che spiegano le crisi di rigetto per i trapianti giuridici (§ 10.2.1), ovvero consigliano di adottare nel vecchio continente il test sulla ragionevole aspettativa di privacy (§ 10.2.2).

Oltre ai criteri processuali per dirimere le controversie dell'ordinamento, i giuristi dispongono nondimeno di ulteriori criteri sostanziali o latamente formali. È sufficiente menzionare nel primo caso, i criteri per mettere alla prova il test sull'aspettativa di privacy, con gli esempi dei pedinamenti digitali, gli obblighi di cancellazione dei dati e le sfide alla privacy informazionale poste dall'autonomia degli agenti artificiali. Anche a tralasciare la pletora di circostanze, in cui i termini generali del discorso giuridico non sembrano aver bisogno d'interpretazione tanto sono automatici (§ 9.3.2), il ricorso sia a principi e clausole generali dell'ordinamento, che a sue disposizioni particolari, permette in molti casi di garantire la certezza del diritto dal punto di vista della sostanza dei problemi affrontati. Prima ancora del test sulla ragionevole aspettativa di privacy, gli esempi di questo approccio sono stati dati dalla risoluzione dei problemi di legalità sollevati dall'uso del design a controllo totale (§ 5.4.3), e con le controversie sull'immunità dei fornitori di servizi in rete, o ISP (§ 8.5.2). Quanto, poi, ai criteri formali, basterà invece accennare a quelli discussi a proposito del principio di tolleranza, nel raffronto con il test di Kant sull'universalità delle massime dell'agire (§ 10.4.4).

Tuttavia, proprio il riferimento al pensiero di Kant sta a ricordare un ulteriore livello di astrazione secondo cui affrontare i diversi ordini di questioni relativi ai motivi del potere nel diritto; vale a dire, prestando attenzione al punto di vista informazionale in chiave semantica, come tale declinabile come vero o falso "sui" diversi stati del mondo. Un conto è, infatti, disporre di un criterio, sulla cui base prendere posizione attorno a una determinata questione giuridica; altra cosa, però, è quella segnalata alla fine del capitolo decimo e che, qui, può essere riassunta con il detto comune ripreso da un'altra opera di Kant, per cui "ciò può essere giusto in teoria, ma non vale per la pratica" [1]. Di pari passo con i criteri normativi messi a punto dal filosofo con i test sull'universalità delle massime dell'agire, o sulla ragionevolezza di ogni legislazione pubblica (§ 5.3.3.1), Kant, quasi a prevenire le successive critiche di Hegel sull'astrattezza del suo metodo, si è preoccupato di rinvenire un fondamento a garanzia della concreta attuabilità delle proprie tesi. A stretto rigore, come si evince dall'opera cui abbiamo più volte fatto cenno, ossia *Per la pace perpetua* (§§ 3.3.2 e 5.3.3), questo fondamento andrebbe rubricato come un tipo d'informazione "come realtà", più che "sulla realtà", stante il peculiare giusnaturalismo del filosofo. Con le sue parole, si può dire che "ciò che fornisce tale garanzia [della pace perpetua] non è altro che la grande artefice Natura […] dal cui corso meccanico scaturisce evidente la finalità di trarre dalle discordie degli uomini, anche contro la loro volontà, la concordia" (Kant ed. 1973: 96).

Anche ad accogliere l'ottimismo della tesi, rimane nondimeno la preoccupazione

[1] Ci siamo già occupati della seconda parte di questo scritto kantiano, ossia il *Contro Hobbes*, nel capitolo quinto (v. infatti § 5.3.3).

kantiana di suffragare le sue idee sul piano reale dell'esistenza, per cui affiora, per ciò stesso, la necessità che Kant si esponga alla verifica sperimentale dei propri assunti. Nel prosieguo dell'argomentazione sul primo supplemento a garanzia della pace perpetua, da cui abbiamo tratto la precedente citazione, Kant dichiara infatti che "come da un lato la natura sapientemente separa i popoli, che la volontà di ogni Stato, anche secondo i principi del diritto internazionale, tenderebbe invece volentieri ad unificare sotto di sé con l'astuzia o con la forza, così d'altro canto essa, facendo leva sul reciproco tornaconto, unisce i popoli che l'idea del diritto cosmopolitico non garantirebbe contro la violenza e la guerra" (*op. cit.*, 101). Con una tesi che sarebbe divenuta oltremodo popolare alla fine del diciannovesimo secolo (v. § 4.2.3), Kant conclude che "è lo spirito commerciale che non può coesistere con la guerra e che prima o poi s'impadronisce d'ogni popolo" (*ibidem*).

Come nel caso di ogni asserzione che verte sulla realtà, più che profilarsi come informazione derivante dalla realtà medesima, secondo gli intendimenti giusnaturalistici di Kant, occorre mettere a confronto l'ipotesi con i dati dell'esperienza. Sebbene, come diremo, il filosofo abbia in parte avuto ragione, bisogna tuttavia segnalare le difficoltà cui va incontro l'idea sullo spirito commerciale come ambasciatore di pace, segnalando, ad esempio, come i due principali obiettivi bellici del Giappone durante la seconda guerra mondiale siano stati tanto la sua principale fonte di materiali da importazione (gli Stati Uniti), quanto il principale mercato per l'esportazione dei propri prodotti (la Cina). In fondo, è stato fatto notare che "siccome la guerra avviene sproporzionatamente tra paesi confinanti, che è al tempo stesso probabile che siano sproporzionatamente partner commerciali, c'è da attendersi che relazioni commerciali e guerra tendano a intrecciarsi" (Diamond 2012: 164).

Tuttavia, a prevenire fraintendimenti, la confutazione empirica della tesi che sia "la forza del denaro […] a promuovere la nobile pace", non comporta abbracciare una tesi eguale e contraria a quella kantiana, nel senso che il diritto sarebbe una semplice variabile dei giochi di potere; come tale, sempre in procinto di ricadere in una condizione di conflitto o di guerra, che sono costanti antropologiche di cui il giurista deve tenere in conto. Altre ricerche empiriche hanno del resto mostrato una sostanziale diminuzione della violenza nelle società contemporanee; per cui, tra i fattori principali del processo, dopo il commercio e lo spirito cosmopolitico kantiano, andrebbero aggiunti l'istruzione e il ruolo svolto dal monopolio legale della forza da parte degli stati (Pinker 2012).

Senza bisogno di entrare nel merito di quest'ultima analisi, la morale da trarsi dal dibattito è sufficientemente chiara. Al fine di comprendere i conflitti e le questioni di potere che si danno nell'esperienza, occorre inserirli in un quadro d'insieme più vasto, come nel caso della natura di Kant, o la sete di vendetta, il sadismo o il tribalismo nel caso di Pinker. Tornando all'indagine sul diritto nell'era delle società ICT-dipendenti, qual è dunque l'ambito più ampio entro cui dar conto delle redistribuzioni di potere che occorrono al loro interno?

*****

È impossibile predire come andrà a finire con la massa dei problemi giuridici elencati in precedenza. Non soltanto, sul piano dell'informazione "come realtà",

non disponiamo di alcun algoritmo che sveli, o anticipi, la loro puntuale risoluzione; ma, anche a disporre, al modo di Dworkin, del criterio per raggiungere in ciascun caso l'unica risposta corretta, questa informazione "per la realtà" non garantirebbe affatto l'esito che avremo "sulla realtà" delle cose.

I problemi giuridici di potere cui abbiamo fatto riferimento, presentano tuttavia, per definizione, un dato in comune; essi, cioè, sono intrecciati al modo in cui il diritto è venuto mutando nell'era della rivoluzione informatica. Sono i profili messi a fuoco fin dal capitolo primo con la figura 3, a proposito del diritto come metatecnologia (§ 1.1.3), e anche con la figura 4, esaminando i processi cognitivi, gli istituti, le tecniche e le istituzioni di questa trasformazione (v. §§ 1.4-1.4.4). Si tratta di un riposizionamento tecnologico successivamente approfondito in ragione dell'accresciuta complessità dei fenomeni da indagare, secondo la cifra prospettica che accomuna sia il mutamento dalle tradizionali forme di governo a quelle dell'odierna governance, sia il passaggio dalla semplicità del modello di Westfalia all'attuale e ben più articolato sistema delle fonti giuridiche: v. in questo caso la figura 5 del capitolo secondo.

Vero è che nessuno dei tre profili della complessità giuridica messi in luce da quest'ultima figura pretende di essere del tutto nuovo: non è così per la nozione di complessità giuridica in termini informazionali che, anzi, abbiamo convenientemente ricondotta al padre del pensiero giuridico e moderno, Thomas Hobbes (§ 2.1.2.1); non è così, nemmeno, per l'idea di complessità giuridica come forma d'emergenza degli ordini spontanei che, per il tramite di Friedrich Hayek, si è fatta risalire al kosmos degli antichi (§ 2.2.1); e non è così, neppure, per la terza e ultima definizione di complessità giuridica come forma d'interdipendenza sistemica e, cioè, come dimensione dei problemi che investono le società nel loro insieme. Basterebbe in tal senso tornare a *Per la pace perpetua*, là dove Kant dichiara che "siccome ora in fatto di associazione (più o meno stretta o larga che sia) di popoli della terra si è progressivamente pervenuti a tal segno, che la violazione del diritto avvenuta in un punto della terra è avvertita in tutti i punti, così l'idea di un diritto cosmopolitico non è una rappresentazione fantasiosa di menti esaltate, ma una necessaria integrazione del codice non scritto […] alla quale solo a questa condizione possiamo lusingarci di approssimarci continuamente" (Kant ed. 1973: 96).

Che cosa c'è dunque di nuovo rispetto a Kant, per cui, lasciando da parte sia la sua ipoteca giusnaturalistica dell'informazione "come realtà", sia il suo progetto giuridico cosmopolitico "per la realtà", occorre prestare attenzione al fatto che ciò che avviene in un punto della terra viene avvertito in tutti gli altri punti?

La risposta, su cui si è insistito lungo tutto il libro, è presto detta: la differenza profonda rispetto ai tempi di Kant è una questione di scala (§§ 2.2.2., 3.1.3.1, 3.3, 4.3.3.1 e 5). Per la prima volta nella storia dell'umanità, non soltanto le organizzazioni sociali impiegano le tecnologie dell'informazione a proprio uso e consumo; ma hanno in realtà cominciato a dipendere dall'impiego di ICT e, in genere, dall'informazione come risorsa vitale. Ciò comporta la creazione di un nuovo mondo, che abbiamo definito come cyberspazio o infosfera, in cui le attività vitali delle società sono progressivamente emigrate. Tanto meno il kantiano "punto della terra" rimane tecnologicamente arretrato e isolato, tanto più la crescente ICT-dipendenza delle odierne società aumenta la natura globale e interconnessa dei problemi da dover af-

frontare. Ma, tanto più i problemi da dover fronteggiare nell'ambito delle società ICT-dipendenti hanno natura sistemica, tanto meno i tradizionali schemi giuridici e politici ereditati dalla tradizione potranno fornire la scala o dimensione adeguata per affrontare questi stessi problemi.

A differenza della Natura di Kant o, se per questo, delle tesi tecno-deterministe esaminate nel capitolo primo, il caso d'internet sta però a ricordare come nulla garantisca l'irreversibilità dei processi in corso. Da un lato, come detto ripetutamente a proposito delle scelte cruciali che avvengono al giorno d'oggi sul piano del design, c'è il rischio, peraltro consumato in Cina e in altri ordinamenti autoritari, di smantellare la rete come l'abbiamo conosciuta agli inizi (§§ 5.2.3 e 5.4.1). D'altro canto, sul fronte occidentale, i fenomeni d'interdipendenza sistemica sembrano tuttavia inevitabili, nel senso che diversi fattori, quali il costo del lavoro nei paesi emergenti o le connesse tendenze demografiche, accentuano la dipendenza delle società occidentali dal loro stesso progresso tecnologico (§ 1.4.4). Di qui, delle due l'una:

– o si rinuncerà allo stato d'interdipendenza sistemica legato all'uso d'ICT e all'informazione come propria risorsa vitale, ma a costo di mettere a rischio lo sviluppo futuro di alcune macroregioni come l'Europa;

– o queste parti del pianeta non potranno che inoltrarsi ulteriormente lungo la strada della ICT-dipendenza, ma al prezzo di imparare a convivere con i problemi giuridici posti dal nuovo scenario.

Definita la sfera di possibilità entro cui pensare lo stesso dover essere delle cose, possiamo di qui far ritorno ai molteplici criteri "per la realtà" di cui dispone il giurista, al fine di orientarci rispetto alle inedite sfide del diritto come meta-tecnologia: basti pensare al plesso di questioni illustrate dalla figura 17 del § 5.3, che dai nodi normativi del design giuridico ha condotto agli odierni dilemmi istituzionali del design.

Il risultato è che l'oggetto del presente volume si profila come forma che media una nuova e complessa interdipendenza attraverso i diversi livelli di governance, con la molteplicità delle sue fonti e in ragione delle tecniche del design. Il diritto nell'era delle società ICT-dipendenti non è insomma che l'interfaccia di queste due novità: la dipendenza informativa che innesca un'inedita interdipendenza sistemica.

# *Riferimenti bibliografici*


Acquisti, A. e Grossklags, J. (2008) *What can behavioral economics teach us about privacy?*, in A. Acquisti e S. Gritzalis (a cura di), *Digital privacy: theory, technologies, and practices*, New York, Auerbach Publications, pp. 363-380.

Allen, A. (1988) *Uneasy access: privacy for women in a free society*, Totowa, N.J., Rowman and Littlefield.

Allen, C., Varner, G. e Zinser, J. (2000) *Prolegomena to any future artificial moral agent*, in "Journal of Experimental and Theoretical Artificial Intelligence", 12, pp. 251-261.

Amin, S. (2000) *The political economy of the twentieth century*, in "Monthly Review", 52, 2, pp. 1-17.

Andronico, A. (2012) *Viaggio al termine del diritto: saggio sulla governance*, Torino, Giappichelli.

Ardia, D.S. (2010) *Free speech savior or shield for scoundrels: an empirical study of intermediary immunity under section 230 of the communications decency act*, in "Loyola of Los Angeles Law Review", 43, 2, pp. 373-505.

Arendt, H. (1989) *Vita activa. La condizione umana*, tr. it., Milano, Bompiani.

Aristotele (2000) *Etica Nicomachea*, tr. it. a cura di C. Mazzarelli, Milano, Bompiani.

Aristotele (2000a) *Metafisica*, tr. it. a cura di G. Reale, Milano, Bompiani.

Augé, M. (2009) *Nonluoghi. Introduzione a un'antropologia della surmodernità*, tr. it., Milano, Elèuthera.

Barabási, A-L. (2004) *Link. La scienza delle reti*, tr. it., Torino, Einaudi.

Beck, U. (2000) *La società del rischio*, tr. it., Roma, Carocci.

Bekey, G.A. (2005) *Autonomous robots: from biological inspiration to implementation and control*, Cambridge, Mass. e Londra, MIT Press.

Benkler, Y. (2007) *La ricchezza della rete. La produzione sociale trasforma il mercato e aumenta le libertà*, tr. it., Milano, Bocconi.

Berners-Lee, T. (1999) *Weaving the web*, San Francisco, Harper.

Berti, E. (1989) *Le ragioni di Aristotele*, Bari, Laterza.

Bevir, M. (2012) *Governance: a very short introduction*, Oxford, Oxford University Press.

Blengino, C. (2012) *I reati informatici*, in M. Durante e U. Pagallo, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet, pp. 219-246.

Bobbio, N. (1938) *L'analogia nella logica del diritto*, Torino, Istituto giuridico.

Bobbio, N. (1977) *Dalla struttura alla funzione: nuovi studi di teoria del diritto*, Milano, Edizioni di Comunità.

Bobbio, N. (1989) *Il terzo assente. Saggi e discorsi sulla pace e la guerra*, Milano, Sonda.

Bobbio, N. (1989a) *Thomas Hobbes*, Torino, Einaudi.

Bodin, J. (1964) *I sei libri dello stato*, vol. I., tr. it. a cura di M. Isnardi Parente, Torino, Utet.

Borruso, R. (1997) *Informatica giuridica*, in "Enciclopedia del diritto", 1997 (aggiornamento), vol. I, pp. 640-677.

Borruso, R. e Tiberi, C. (2001) *L'informatica per il giurista. Dal bit a Internet*, Milano, Giuffrè.
Boulet, R., Mazzega, P. e Bourcier, D. (2010) *Network analysis of the French environment code*, in P. Casanovas, U. Pagallo, G. Sartor e G. Ajani (a cura di), *AI approaches to the complexity of legal systems: AICOL I-II*, Dordrecht, Springer, pp. 39-53.
Boyd, D. (2010) *Social networks sites as networked publics: affordances, dynamics, and implications*, in Z. Papacharissi (a cura di), *Networked self: identity, community, and culture on social networks sites*, Londra, Routledge, pp. 39-58.
Bradford, A. (2012) *The Brussels effect*, in "Northwestern University Law Review", 107, 1, pp. 1-68.
Breazeal, C. (2002) *Designing sociable robots*, Cambridge, Mass., MIT Press.
Brey, P. (2010) *Values in technology and disclosive computer ethics*, in L. Floridi (a cura di), *Information and computer ethics*, Cambridge, UK, Cambridge University Press, pp. 41-58.
Brooks, R.A. (2013) *Moore's law*, in J. Brockman (a cura di), *This explains everything*, New York, Harper, pp. 236-238.
Bull, H. (1977) *The anarchical society: a study of order in world politics*, Londra, MacMillan.
Bygrave, L.A. (2012), *Contract versus statute in internet governance*, in I. Brown (a cura di), *Research handbook on governance of the internet*, Cheltenham, Elgar, pp. 168-197.

Calasso, F. (1957) *I glossatori e la teoria della sovranità. Studio di diritto comune pubblico*, Milano, Giuffrè.
Cate, F.H. e Mayer-Schönberger, V. (2013) *Data use and impact global workshop*, The Center for Information Policy Research, 1° dicembre, Indiana, The Trustees of Indiana University.
Caterina, R., a cura di (2008) *I fondamenti cognitivi del diritto*, Milano, Mondadori.
Cavoukian, A. (2010) *Privacy by design: the definitive workshop*, in "Identity in the Information Society", 3, 2, pp. 247-251.
Cerf, V., Ryan, P. e Senges, M. (2013) *Internet governance is our shared responsibility*, in corso di pubblicazione presso il "Journal of Law and Policy for the Information Society", 10 ISJLP_(2014), ma disponibile su *www.ssrn* dal 13 agosto 2013.
Chaitin, G. (2005) *Teoria algoritmica della complessità*, tr. it., Torino, Giappichelli.
Chandler, S. (2005) *The network structure of supreme court jurisprudence*, in "University of Houston Law Center", 2005-W-01.
Cicerone, M.T. (1974) *Opere politiche e filosofiche*, tr. it. a cura di L. Ferrero e N. Zorzetti, vol. I, Torino, Utet.
Cohen-Almagor, R. (2010), *Responsibility of and trust in ISPs*, in "Knowledge, Technology & Policy", 23, 3-4, pp. 381-397.
Coing, H. (1989) *Von Bologna bis Brüssels: Europäische Gemeinsamkeit, Gegenwart und Zukunft*, Kölner Juristische Gesellschaft, vol. IX, Colonia, Bergish Gladbach.
Cole, D. (2014) *Can privacy be saved?*, in "The New York Review of Books", 6 marzo.
Collingridge, D. (1980) *The social control of technology*, New York, St. Martin's Press e Londra, Pinter.
Crisafulli, V. (1976), *Costituzione*, in "Enciclopedia del Novecento", vol. I, pp. 1030-1061.

Damasio, A. (2012) *Self comes to mind. Constructing the conscious brain*, New York, Vintage.
Danforth Zeronda, N. (2010) *Street shootings: covert photography and public privacy*, in "Vanderbilt Law Review", 63, pp. 1131-1159.
Dautenhahn, K. (2007) *Socially intelligent robots: dimensions of human-robot interaction*, in "Philosophical Transactions of the Royal Society B: Biological Sciences", 362, 1480, pp. 679-704.

Davis, M. (2003) *Il calcolatore universale*, tr. it., Milano, Adelphi.
Delazay, Y. e Garth, B. (1996) *Dealing with virtue: international commercial arbitration and the construction of a transnational legal order*, Chicago, University of Chicago Press.
Dennett, D. (1987) *The intentional stance*, Cambridge, Mass., MIT Press.
Diamond, J. (2012) *The world until yesterday*, Londra, Penguin.
Doorn, N. e Hansson, S. (2011) *Should probabilistic design replace safety factors?*, in "Philosophy and Technology", 24, 2, pp. 151-168.
Dunn, J. (1992) *Il pensiero politico di John Locke*, tr. it., Bologna, Il Mulino.
Durante, M. (2007) *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Torino, Giappichelli.
Durante, M. e Pagallo, U., a cura di (2012) *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet.
Dworkin, R. (1985) *A matter of principle*, Oxford, Oxford University Press (tr. it., *Questioni di principio*, Milano, Il Saggiatore).
Dworkin, Ronald (1986) *Law's empire*, Cambridge, Mass., Harvard University Press (tr. it., *L'impero del diritto*, Milano, Il Saggiatore).

Etzioni, A. (2004) *How patriotic is the patriot act? Freedom versus security in the age of terrorism*, New York-Londra, Routledge.
Euchner, W. (1976) *La filosofia politica di Locke*, tr. it., Bari, Laterza.

Flanagan, M., Howe, D.C. e Nissenbaum, H. (2008) *Embodying values in technology: theory and practice*, in J. van den Hoven e J. Weckert (a cura di), *Information technology and moral philosophy*, New York, Cambridge University Press, pp. 322-353.
Floridi, L. (2005) *La filosofia dell'informazione e i suoi problemi*, in "Iride", XVIII, 45, pp. 291-312.
Floridi, L. (2006) *Four challenges for a theory of informational privacy*, in "Ethics and Information Technology", 8, 3, pp. 109-119.
Floridi, L. (2008) *Information ethics, its nature and scope*, in J. van den Hoven e J. Weckert (a cura di), *Moral philosophy and information technology*, Cambridge, Cambridge University Press, pp. 40-65.
Floridi, L. (2009) *Infosfera: etica e filosofia nell'età dell'informazione*, tr. it., Torino, Giappichelli.
Floridi, L. (2012) *La rivoluzione dell'informazione*, tr. it., Torino, Codice.
Floridi, L. (2014) *The rise of the MASs*, in L. Floridi (a cura di), *Protection of information and the right to privacy - a new equilibrium?*, Dordrecht, Springer, pp. 95-122.
Floridi, L. (2014a) *The fourth revolution*, Oxford, Oxford University Press.
Floridi, L., a cura di (2014) *The onlife manifesto: being human in a hyperconnected era*, Dordrecht, Springer.
Fowler, J.H. e Jeon, S. (2008) *The authority of supreme court precedent*, in "Social Networks", 30, pp. 16-30.
Fried, Ch. (1990) *Privacy: a rational context*, in M.D. Ermann, M.B. Williams e C. Gutierrez (a cura di), *Computers, ethics, and society*, New York, Oxford University Press, pp. 50-63.
Fuller, L.L. (1969) *The morality of law*, New Haven, Conn., Yale University Press.

Gadamer, H.G. (1984) *Studi platonici*, volume secondo, tr. it., Casale Monferrato, Marietti.
Garfinkel, S. e Spafford, G. (1997), *Web security & commerce*, Sebastopol, O'Reilly.

Garthoff, J. (2010) *Legitimacy is not authority*, in "Law and Philosophy", 29, 6, pp. 669-694.
Gavison, R. (1980) *Privacy and the limits of the law*, in "Yale Law Journal", 89, pp. 421-471.
Glorioso, A. (2012) *Un nuovo concetto di "auto-determinazione informazionale" come bussola concettuale per navigare il nuovo mondo digitale*, in M. Durante e U. Pagallo, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet, pp. 383-394.
Glorioso, A., Pagallo, U. e Ruffo, G. (2010) *The social impact of P2P systems*, in X. Shen, H. Yu, J. Buford e M. Akon (a cura di), *Handbook of peer-to-peer networking*, Dordrecht, Springer, pp. 47-70.
Goldsmith, J. (1998) *Against cyberanarchy*, in "University of Chicago Law Review", 65, pp. 1199-1250.
Goldsmith, J. e Wu, Th. (2006) *Who controls the internet: illusions of a borderless world*, New York, Oxford University Press.
Gordley, James (2006) *Foundations of private law: property, tort, contract, unjust enrichment*, Oxford-New York, Oxford University Press.
Graziadei, M. (2009) *Legal transplants and the frontiers of legal knowledge*, in "Theoretical Inquiries in Law", 10, 2, pp. 723-743.
Grindle, M. (2007) *Good enough governance revisited*, in "Development Policy Review", 25, 5, pp. 533-574.

Habermas, J. (1995) *Fatti e norme: contributi a una teoria discorsiva del diritto e della democrazia*, tr. it., Milano, Guerini.
Halliday, T.C. e Osinsky, P. (2006) *Globalization of law*, in "Annual Review of Sociology", 32, pp. 447-470.
Hart, H.L.A. (1991) *Il concetto di diritto*, tr. it., Torino, Einaudi.
Hart, H.L.A. (1994) *The concept of law*, Oxford, Clarendon (seconda edizione).
Hayek, F.A. (1986) *Legge, legislazione e libertà: una nuova enunciazione dei principi liberali della giustizia e della economia politica*, tr. it., Milano, Il Saggiatore.
Hayek, F.A. (1999) *La società libera*, tr. it., Milano, Seam.
Hildebrandt, M. (2011) *Legal protection by design: objections and refutations*, in "Legisprudence", 5, pp. 223-248.
Hobbes, Th. (1992) *Leviatano,* tr. it. a cura di A. Pacchi, Roma-Bari, Laterza.
Holtzmann, D.H. (2006) *Privacy lost: how technology is endangering your privacy*, San Francisco, Jossey-Bass.
Hörnle, J. (2009) *The jurisdictional challenge of the internet*, in L. Edwards e Ch. Waelde (a cura di), *Law and the internet*, Oxford, Hart, pp. 121-158.

Jarfinkel, S. (2000) *Database nation: the death of privacy in the 21st century*, Sebastopol, O'Reilly.
Jessup, P.C. (1956), *Transnational law*, New Haven, Yale University Press.
Jobs, S. (2007) *Thoughts on music*, in *http://www.apple.com/hotnews/thoughtsonmusic/* (ultimo accesso 30 maggio 2014).

Kallinikos, J. (2006) *The consequences of information: institutional implications of technological change*, Cheltenham, UK e Northampton, Mass., Elgar.
Kaminski, M.E. (2013) *Drone federalism: civilian drones and the things they carry*, in "California Law Review Circuit", 4, pp. 57-74.
Kant, I. (1969) *Fondamenti della metafisica dei costumi*, tr. it. a cura di E. Carrara, Firenze, La nuova Italia.

Kant, I. (1973) *Lo stato di diritto*, tr. it. a cura di N. Merker, Roma, Editori Riuniti.
Kant, I. (2004) *Critica del giudizio*, tr. it. a cura di M. Marassi, Milano, Bompiani.
Kaufmann, D. (2003) *Rethinking governance: empirical lessons challenge orthodoxy*, Washington, DC, Banca Mondiale.
Kaza, S., Xu, J., Marshall, B. e Chen, H. (2005) *Topological analysis of criminal activity networks in multiple jurisdictions*, in "Proceedings of the 2005 National Conference on Digital Government Research", pp. 251-252.
Kelly, K. (2011) *Quello che vuole la tecnologia*, tr. it., Torino, Codice.
Kelsen, H. (1952) *Dottrina pura del diritto* (prima edizione 1934), tr. it., Torino, Einaudi.
Kelsen, H. (1959) *Teoria generale del diritto e dello stato*, tr. it., Milano, Edizioni di Comunità.
Kelsen, H. (1966) *Dottrina pura del diritto* (edizione 1960), tr. it., Torino, Einaudi.
Kelsen, H. (1981) *La giustizia costituzionale*, tr. it., Milano, Giuffrè.
Kelsen, H. (1989) *Il problema della sovranità e la teoria del diritto internazionale. Contributo per una dottrina pura del diritto*, tr. it., Milano, Giuffrè.
Kerr, O. (2004) *The fourth amendment and new technologies: constitutional myths and the case for caution*, in "Michigan Law Review", 102, pp. 801-888.
Kesan, J.P. e Shah R.C. (2006) *Setting software defaults: perspectives from law, computer science and behavioural economics*, in "Notre Dame Law Review", 82, pp. 583-634.
Koops, B.J. (2006) *Should ICT regulation be technology-neutral?*, in B.J. Koops e al. (a cura di), *Starting points for ICT regulation: deconstructing prevalent policy one-liners*, L'Aia, TMC Asser, pp. 77-108.
Kurzweil, R. (2008) *La singolarità è vicina*, tr. it., Milano, Apogeo.

Lee-Makiyama, H. (2014) *The political economy of data: EU privacy regulation and the international redistribution of its costs*, in L. Floridi (a cura di), *Protection of information and the right to privacy - a new equilibrium?*, Dordrecht, Springer, pp. 85-94.
Lessig, L. (1999) *Code and other laws of cyberspace*, New York, Basic Books.
Lessig, L. (2004) *Free culture: the nature and future of creativity*, New York, Penguin Press.
Levy, D. (2007) *Love and sex with robots: the evolution of human-robot relationships*, New York, Harper.
Linarelli, J. (2009) *Analytical jurisprudence and the concept of commercial law*, in "Pennsylvania State Law Review", 114, pp. 119-215.
Livio, T. (1979) *Storie*, tr. it. a cura di L. Perelli, libri I-V, Torino, Utet.
Lloyd, S. (2006) *Il programma dell'universo*, tr. it., Torino, Einaudi.
Locke, J. (2009) *Il secondo trattato sul governo*, tr. it. a cura di A. Gialluca, Milano, BUR.
Lockton, D., Harrison, D.J. e Stanton, N.A. (2010) *The design with intent method: a design tool for influencing user behaviour*, in "Applied Ergonomics", 41, 3, pp. 382-392.
Lolli, G. (2002) *Filosofia della matematica. L'eredità del Novecento*, Bologna, Il Mulino.
Lolli, G. e Pagallo, U., a cura di (2008) *La complessità di Gödel*, Torino, Giappichelli.
Lombardi, G. (1987) *Lo stato federale: profili di diritto comparato*, Torino, Giappichelli.
Luhmann, N. (1978) *Sistema giuridico e dogmatica giuridica*, tr. it., Bologna, Il Mulino.
Luhmann, N. (1990) *Sistemi sociali. Fondamenti di una teoria generale*, tr. it., Bologna, Il Mulino.

Mackenzie, D. e Wajcman, J. (1985) *The social shaping of technology*. Milton Keynes, UK, Open University Press.

MacKinnon, R. (2012) *Consent of the networked: the worldwide struggle for internet freedom*, New York, Basic Books.
Malmgren, S. (2011) *Towards a theory of jurisprudential relevance ranking: using link analysis on EU case law*, tesi per il master in diritto presso l'Università di Stoccolma.
Matteucci, N., a cura di (1962) *Antologia dei costituzionalisti inglesi*, Bologna, Il Mulino.
Mayer-Schönberger, V. (2008) *Demystifying Lessig*, in "Wisconsin Law Review", 4, pp. 713-746.
McDaniels, T. e Small, M.J. (2004) *Risk analysis and society*, Cambridge, Cambridge University Press.
McIlwain, Ch.H. (1990) *Costituzionalismo antico e moderno*, tr. it., Bologna, Il Mulino.
Moor, J.H. (1997), *Towards a theory of privacy in the information age*, in "Computers and Society", 27, 3, pp. 27-32.
Moravec, H. (1999) *Robot: mere machine to transcendent mind*, Londra, Oxford University Press.
Murray, A.D. (2007) *The regulation of cyberspace: control in the online environment*, New York, Routledge-Cavendish.

Newman, A. (2008) *Protectors of privacy: regulating personal data in the global economy*, Ithaca, New York, Cornell University Press.

Ohm, P. (2009) *Broken promises of privacy: responding to the surprising failure of anonymisation*, in "UCLA Law Review", 57, 6, pp. 1701-1777.
Orito, Y. e Murata, K. (2007) *Rethinking the concept of information privacy: a Japanese perspective*, in T.W. Bynum, K. Murata e S. Rogerson (a cura di), *Glocalisation: bridging the global nature of information and communication technology and the local nature of human beings*, Tokyo, Ethicomp, pp. 448-455.

Pagallo, U. (2002) *Alle fonti del diritto: mito, scienza, filosofia*, Torino, Giappichelli.
Pagallo, U. (2004) *Introduzione* a F. Bergadano, A. Mantelero, G. Ruffo e G. Sartor, *Privacy digitale: giuristi e informatici a confronto*, Torino, Giappichelli.
Pagallo, U. (2005) *Introduzione alla filosofia digitale: da Leibniz a Chaitin*, Torino, Giappichelli.
Pagallo, U. (2008) *La tutela della privacy tra Stati Uniti ed Europa: modelli giuridici a confronto*, Milano, Giuffrè.
Pagallo, U. (2009) *Sul principio di responsabilità giuridica in rete*, in "Il diritto dell'informazione e dell'informatica", XXV, 4-5, pp. 705-734.
Pagallo, U. (2011) *ISPs & rowdy web sites before the law: should we change today's safe harbour clauses?*, in "Philosophy and Technology", 24, 4, pp. 419-436.
Pagallo, U. (2012) *Cracking down on autonomy: three challenges to design in IT law*, in "Ethics and Information Technology", 14, 4, pp. 319-328.
Pagallo, U. (2012a) *On the principle of privacy by design and its limits: technology, ethics, and the rule of Law*, in S. Gutwirth et al. (a cura di), *European data protection: in good health?*, Dordrecht, Springer, pp. 331-346.
Pagallo, U. (2013) *The laws of robots: crimes, contracts, and torts*, Dordrecht, Springer.
Pagallo, U. (2013a) *Robots in the cloud with privacy: a new threat to data protection?*, in "Computer Law & Security Review", 29, 5, pp. 501-508.
Pagallo, U. (2014) *Good onlife governance: on law, spontaneous orders, and design*, in L. Floridi (a cura di), *The onlife manifesto: being human in a hyperconnected era*, Dordrecht, Springer.
Pagallo, U. e Bassi, E. (2013) *Open data protection: challenges, perspectives, and tools for the reuse*

*of PSI*, in M. Hildebrandt, K. O'Hara e M. Waidner (a cura di), *Digital enlightenment yearbook 2013*, Amsterdam, IOS Press, pp. 179-189.

Pagallo, U. e Bassi, E. (2011) *The future of EU working parties' "the future of privacy" and the principle of privacy by design*, in M. Bottis (a cura di), *An information law for the 21st century*, Atene, Nomiki Bibliothiki Group, pp. 286-309.

Pagallo, U. e Durante, M. (2009) *Three roads to P2P systems and their impact on business ethics*, in "Journal of Business Ethics", 90, 4, pp. 551-564.

Pagallo, U. e Durante, M. (2013) *Diritto, memoria ed oblio*, in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, Giappichelli, pp. 65-84.

Pagallo, U. e Durante, M. (2014) *Legal memories and the right to be forgotten*, in L. Floridi (a cura di), *Protection of information and the right to privacy - a new equilibrium?*, Dordrecht, Springer, pp. 17-30.

Pagallo, U. e Ruffo, G. (2007) *P2P systems in legal networks: another "small world" case*, in "Eleventh International Conference on Artificial Intelligence and Law", Stanford, ACM, pp. 287-288.

Pagallo, U. e Ruffo, G. (2012) *Peer-to-peer*, in M. Durante e U. Pagallo, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet, pp. 487-508.

Paladin, L. (1996) *Le fonti del diritto italiano*, Bologna, Il Mulino.

Parris, R. (2012) *Online T&Cs longer than Shakespeare plays – who reads them?*, in "Which? Conversation", 23 marzo, in *http://conversation.which.co.uk/technology/length-of-website-terms-and-conditions/*.

Pinch, T.J. e Bijker, W.E. (1987) *The social construction of facts and artifacts, or, how the sociology of science and the sociology of technology might benefit each other*, in W.E. Bijker, T.J. Pinch e T.P. Hughes (a cura di), *The social construction of technological systems*, Cambridge, MA, The MIT Press, pp. 17-50.

Pinelli, C. (2009) *Forme di stato e forme di governo: corso di diritto costituzionale comparato*, Napoli, Jovene.

Pinker, S. (2007) *The stuff of thought: language as a window into human nature*, New York, Viking.

Pinker, S. (2012) *The better angels of our nature*, New York, Penguin.

Platone (1993) *Fedro*, tr. it. a cura di G. Reale, Milano, Rusconi.

Platone (2000) *La Repubblica*, tr. it. a cura di F. Sartori, Roma-Bari, Laterza.

Popper, K.R. (2002) *La società aperta e i suoi nemici*, tr. it., Roma, Armando.

Posner, R. (1973) *Economic analysis of law*, Boston, Little Brown.

Posner, R. (1988) *The jurisprudence of skepticism*, in "Michigan Law Review", 86, 5, pp. 827-891.

Post, D. (2009) *In search of Jefferson's moose: notes on the state of cyberspace*, New York, Oxford University Press.

Potter, N. (2010) *Cos'è un designer*, tr. it., Torino, Codice.

Prosser, W. (1960) *Privacy*, in "California Law Review", 48, 3, pp. 383-423.

Rawls, J. (1971) *A theory of justice*, Cambridge, Mass., Belknap Press (tr. it. Milano, Feltrinelli, 1982).

Ricoeur, P. (2004) *Ricordare, dimenticare, perdonare. L'enigma del passato*, tr. it., Bologna, Il Mulino.

Robilant, E. di (1973) *Il diritto nella società industriale*, in "Rivista internazionale di filosofia del diritto", LI, pp. 225-262.

Reed, Ch. (2012) *Making laws for cyberspace*, Oxford, Oxford University Press.

Rodotà, S. (2005) *Intervista su privacy e libertà*, Roma-Bari, Laterza.
Rodotà, S. (2006) *The retention of electronic communication traffic data*, in "Revista d'Internet, Dret I Política", 3, pp. 53-60.
Rosenau, J.M. e Czempiel, E.O. (1992) G*overnance without government: order and change in world politics*, Cambridge, Cambridge University Press.
Rousseau, J.-J. (1997) *Il contratto sociale*, tr. it. a cura di V. Gerratana, Torino, Einaudi.
Ruffo, G. (2012) *Rete e reti*, in M. Durante e U. Pagallo, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet, pp. 20-44.

Sacco, R. (2007) *Antropologia giuridica*, Bologna, Il Mulino.
Sartor, G. e Viola de Azevedo Cunha, M. (2010) *The Italian Google-case: privacy, freedom of speech and responsibility of providers for user-generated contents*, in "International Journal of Law, Information and Technology", 18, 4, pp. 356-378.
Schmidt, E. e Cohen, J. (2013) *The new digital age*, Londra, John Murray.
Schmitt, C. (1981) *Il custode della costituzione*, tr. it., Milano, Giuffrè.
Schmitt, C. (1991) *Il nomos della terra nel diritto internazionale dello 'jus publicum europaeum'*, tr. it., Milano, Adelphi.
Schultz, Th. (2007) *Private legal systems: what cyberspace might teach legal theorists*, in "Yale Journal of Law and Technology", 10, pp. 151-193.
Schwartz, P.M. (2013) *The EU-US privacy collision: a turn to institutions and procedures*, in "Harvard Law Review", 126, pp. 1966-2009.
Senor, M. (2012) *Videoriprese di immagini non comunicative: un vuoto legislativo che la giurisprudenza non intende colmare con un'interpretazione garantista*, in "Penale.it", reperibile in *http://www.penale.it/stampa.asp?idpag=1079* (ultimo accesso 30 maggio 2014).
Shannon, C. e Wiener, W. (1971) *La teoria matematica delle comunicazioni*, tr. it., Milano, Etas.
Slaughter, A.M. (2004) *A new world order: government networks and the disaggregated state*, Princeton, Princeton University Press.
Smith, A. (1978) *Lectures on jurisprudence*, Indianapolis, Liberty Class.
Solove, D.J. (2013) *Privacy self-management and the consent paradox*, in "Harvard Law Review", 126, 7, pp. 1880-1903.
Solum, L.B. (2009) *Models of internet governance*, in L.A. Bygrave e J. Bing (a cura di), *Internet governance: infrastructure and institutions*, New York, Oxford University Press, pp. 48-91.
Simon, H.A. (1996) *The sciences of the artificial*, Cambridge Mass. e Londra, MIT Press.
Singer, P. (2009) *Wired for war: the robotics revolution and conflict in the 21st century*, Londra, Penguin.
Sykes, C. (1999) *The end of privacy: the attack on personal rights at home, at work, on-line, and in court*, New York, St. Martin's Griffin.

Talmon, J.L. (2000) *Le origini della democrazia totalitaria*, tr. it., Bologna, Il Mulino.
Tavani, H.T. (2007) *Philosophical theories of privacy: implications for an adequate online privacy policy*, in "Metaphilosophy", 38, 1, pp. 1-22.
Teubner, G. (2007) *Breaking frames: the global interplay of legal and social systems*, in "American Journal of Comparative Law", 45, pp. 145-169.
Thaler, R.H. e Sunstein, C.R. (2009) *La spinta gentile. La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, tr. it., Milano, Feltrinelli.
Tribe, L.H. (1988) *American constitutional law*, Mineola, New York, Foundation Press.
Turing, A.M. (1950) *Computing machinery and intelligence*, in "Mind", 49, pp. 433-460.

Vitale, E. (2008) *La società civile tra impotenza e strapotere: qualche riflessione su 'governance' e democrazia*, in "Teoria politica", 2, pp. 31-39.

Waltz, K. (1987), *Teoria della politica internazionale*, tr. it., Bologna, Il Mulino.
Warren, S. e Brandeis, L. (1890) *The right to privacy*, in "Harvard Law Review", 14, pp. 193-220.
Watson, A. (1974) *Legal transplants: an approach to comparative law*, Edimburgo e Londra, Scottish Academic Press.
Watts, D.J. e Strogatz, S.H. (1998) *Collective dynamics of "small-world" networks*, in "Nature", 393, pp. 440-442.
Weil, E. (1990) *Aristotelica*, tr. it., Milano, Guerini.
Westin, A.F. (1967) *Privacy and freedom*, New York, Atheneum Press.
Whitehead, A.N. e Russell, B. (1960) *Principia mathematica*, vol. I, Cambridge, Cambridge University Press.
Wiener, N. (1950) *The human use of human beings: cybernetics and society*, New York, Doubleday.
Winkels, R. e de Ruyter, J. (2012) *Survival of the fittest: network analysis of Dutch supreme court cases*, in M. Palmirani, U. Pagallo, P. Casanovas e G. Sartor (a cura di), *AI approaches to the complexity of legal systems: AICOL III*, Dordrecht, Springer, pp. 106-115.
Winn, P. (2009) *Katz and the origins of the "reasonable expectation of privacy" test*, in "McGeorge Law Review", 40, 1, pp. 1-12.
Wright, S. (2005) *The echelon trail: an illegal vision*, in "Surveillance and Society", 3, 2-3, pp. 198-215.

Yeung, K. (2007) *Towards an understanding of regulation by design*, in R. Brownsword e K. Yeung (a cura di), *Regulating technologies: legal futures, regulatory frames and technological fixes*, Londra, Hart, pp. 79-108.

Zittrain, J. (2007) *Perfect enforcement on tomorrow's internet*, in R. Brownsword e K. Yeung (a cura di), *Regulating technologies: legal futures, regulatory frames and technological fixes*, Londra, Hart, pp. 125-156.
Zumbansen, P. (2006) *Transnational law*, in J. Smits (a cura di), *Encyclopedia of comparative law*, Cheltenham, Elgar, pp. 738-754.

# DIGITALICA

*Collana diretta da* UGO PAGALLO

## Volumi pubblicati

1. UGO PAGALLO, *Introduzione alla filosofia digitale. Da Leibniz a Chaitin*, 2005, pp. VIII-164.

2. FRANCESCO BERGADANO, ALESSANDRO MANTELERO, GIANCARLO RUFFO, GIOVANNI SARTOR, *Privacy digitale. Giuristi e informatici a confronto*, 2005, pp. IV-100.

3. GREGORY J. CHAITIN, *Teoria algoritmica della complessità.* Presentazione di John Casti, 2006, pp. IV-112.

4. UGO PAGALLO, *Teoria giuridica della complessità. Dalla "polis primitiva" di Socrate ai "mondi piccoli" dell'informatica*. *Un approccio evolutivo*, 2006, pp. VIII-280.

5. MASSIMO DURANTE, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, 2007, pp. XIV-326.

6. CRISTIAN S. CALUDE, CARLO CELLUCCI, GREGORY J. CHAITIN, MAURIZIO FERRARIS, GABRIELE LOLLI, UGO PAGALLO, GIOVANNI SAMBIN, CARLO TOFFALORI*, La complessità di Gödel*, a cura di Gabriele Lolli e Ugo Pagallo, 2008, pp. VI-174.

7. ANTONELLA ARDIZZONE, LORENZO BENUSSI, CARLO BLENGINO, ANDREA GLORIOSO, GIOVANNI B. RAMELLO, GIANCARLO RUFFO, MASSIMO TRAVOSTINO*, Copyright digitale. L'impatto delle nuove tecnologie tra economia e diritto*. Presentazione di Marco Ricolfi, 2009, pp. VI-190.

8. LUCIANO FLORIDI, *Infosfera. Etica e filosofia nell'età dell'informazione*. Introduzione di Terrell Ward Bynum, 2009, pp. X-234.

9. RUTH CHADWICK, RAPHAEL CUIR, FRANCESCA GIGLIO, DAVID LYON, ANTONIO MARTURANO, MARK POSTER, ANDREA RESCA, MONICA SENOR, ANTONIO SPAGNOLO, SARAH WILSON, *Il Corpo Digitale: natura, informazione, merce*, a cura di Antonio Marturano, 2010, pp. XVI-168.

10. FRANCESCO ROMEO, *Lezioni di logica ed informatica giuridica*, 2012, pp. X-246.

11. MASSIMILIANO CARRARA, DANIELE CHIFFI, CIRO DE FLORIO, ALFREDO DI GIORGIO, ANDREA FAVARO, SILVIA GAIO, SERGIO GALVAN ANTONIO NEGRO, CARLO PENCO, DAVIDE SERGIO, *Prova e giustificazione*, a cura di Alfredo Di Giorgio e Daniele Chiffi, 2013, pp. VI-266.

12. UGO PAGALLO, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, 2014, pp. XXIV-360.

**Fin dall'inizio della storia, le società umane hanno fatto uso delle tecnologie dell'informazione e comunicazione (ICT); a partire dalla fondamentale, la scrittura. Per la prima volta nella storia dell'umanità, le società contemporanee dipendono tuttavia dalle ICT e, in generale, dall'informazione come propria risorsa vitale. Il presente volume spiega come i sistemi giuridici siano venuti riposizionandosi di fronte alle profonde trasformazioni in atto. Ciò vale sia riguardo alle autorità che ai fattori di produzione normativa dell'ordinamento, come anche all'intento di reagire alle sfide della rivoluzione tecnologica con le armi stesse della tecnologia. Un esempio di scuola per cogliere questo mutamento in termini di governance, fonti del diritto e design normativo e istituzionale, è dato dalla protezione dei dati personali e con la tutela della privacy. Il diritto nell'età dell'informazione non è infatti che l'interfaccia che media queste due sfere: una nuova dipendenza tecnologica che innesca un'inedita interdipendenza sistemica.**

**UGO PAGALLO è ordinario di filosofia del diritto presso il dipartimento di Giurisprudenza dell'Università di Torino. Membro del gruppo di ricerca europeo RPAS *Steering* sui droni civili (2011-2012), del gruppo di esperti istituito dalla Commissione europea DG-INFSO per il progetto *Onlife* (2012-2013), nonché del comitato etico del progetto Caper entro il settimo programma quadro di ricerca e sviluppo tecnologico dell'Unione europea (2013-2014), è *Faculty* del CTLS di Londra e co-dirige la collana AICOL per la *Springer*, su intelligenza artificiale, complessità e sistemi giuridici. Autore di numerose pubblicazioni nelle più prestigiose riviste internazionali dei settori in cui verte la sua ricerca, come la teoria delle reti e la robotica, la teoria generale del diritto e l'etica dell'informazione, insieme ad alcuni istituti chiave del diritto delle nuove tecnologie come la privacy informazionale, questa è la decima monografia.**

ISBN/EAN
9 788834 858356